

# Fault-tolerant ancilla preparation and noise threshold lower bounds for the 23-qubit Golay code

Adam Paetznick\*

Ben W. Reichardt\*

## Abstract

In fault-tolerant quantum computing schemes, the overhead is often dominated by the cost of preparing codewords reliably. This cost generally increases quadratically with the block size of the underlying quantum error-correcting code. In consequence, large codes that are otherwise very efficient have found limited fault-tolerance applications. Fault-tolerant preparation circuits therefore are an important target for optimization.

We study the Golay code, a 23-qubit quantum error-correcting code that protects the logical qubit to a distance of seven. In simulations, even using a naïve ancilla preparation procedure, the Golay code is competitive with other codes both in terms of overhead and the tolerable noise threshold. We provide two simplified circuits for fault-tolerant preparation of Golay code-encoded ancillas. The new circuits minimize error propagation, reducing the overhead by roughly a factor of four compared to standard encoding circuits. By adapting the malignant set counting technique to depolarizing noise, we further prove a threshold above  $1.32 \times 10^{-3}$  noise per gate.

## 1 Introduction

A main obstacle to building a quantum computer is handling noise. The fault-tolerance threshold theorem [AB97, Kit97] implies that reliable quantum computation is possible in principle. So long as the noise is weak enough, the probability that a computation executes correctly can be made arbitrarily close to one at the cost of increased circuit complexity, i.e., overhead. Fault-tolerant quantum circuit constructions typically aim to maximize the tolerable noise rate while maintaining modest overhead.

A quantum fault-tolerance scheme generally works by encoding data into a quantum error-correcting code and alternating steps of fault-tolerant computation and error correction (Figure 1). The error-correction step, intended for recovery from accumulated noise, is normally much more complicated than the computation step. Therefore error correction is the dominant factor in determining the scheme’s resource overhead, and is usually the major bottleneck in determining the highest tolerable noise rate or “noise threshold.” In particular, the details of how error correction is implemented are more important than the properties of the underlying quantum error-correcting code.

For example, with the nine-qubit Bacon-Shor code, a fault-tolerant logical controlled-not (CNOT) gate between two code blocks can be implemented using nine physical CNOT gates, whereas an optimized error-correction method uses 24 physical CNOT gates [AC07]. For larger quantum error-correcting codes, the asymmetry between computation and error correction is greater still.

---

\*School of Computer Science and Institute for Quantum Computing, University of Waterloo

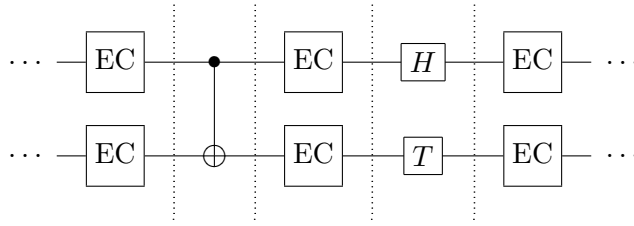


Figure 1: The circuit fragment above shows an example of alternating rounds of fault-tolerant error-correction (EC) and computation. The wires represent encoded data blocks and the gate symbols (CNOT, H, T) represent encoded operations.

With the 23-qubit Golay code, a fault-tolerant logical CNOT gate requires only 23 physical CNOT gates, whereas a standard error-correction method uses 2400 physical CNOT gates.

Larger quantum error-correcting codes, with higher distance and possibly higher rates, can still outperform smaller codes. Separate numerical studies by Steane [Ste03] (see also [Ste07]) and Cross, DiVincenzo and Terhal [CDT09] have each compared fault-tolerance schemes based on a variety of codes. They identify larger codes that, compared to the seven-qubit Steane code and the nine-qubit Bacon-Shor code, can tolerate higher noise rates with comparable resource requirements. In particular, their estimates single out the Golay code as a top performer.

We give an optimized fault-tolerant error-correction procedure for the Golay code that uses only 640 CNOT gates. Our derivation is based on two main ideas. First, we simplify Steane’s Latin-rectangle-based scheme for preparing encoded  $|0\rangle$  states [Ste02], by taking advantage of overlaps between the code’s stabilizers. Second, we reduce the overall number of encoded  $|0\rangle$  states required for error correction by carefully tracking the exact propagation of errors. Both ideas are generally applicable to other large quantum error-correcting codes.

We then prove a lower bound on the threshold for depolarizing noise of  $1.32 \times 10^{-3}$  noise per gate. This result is an order of magnitude improvement over the best previous lower bound for the Golay code [AC07] based on an adversarial noise model. It is also about 25 percent better than the lower bound due to [AGP08] based on a stochastic noise model slightly stronger than ours, but for a dramatically different fault-tolerance scheme. Our proof uses malignant set counting [AGP06], extensively tailored for our specific error correction circuits and for depolarizing noise. Instead of assuming adversarial noise at higher levels of code concatenation, the counting procedure keeps track of multiple types of malignant events to create a transformed stochastic noise model for each level, allowing for a more accurate analysis.

## 1.1 Fault-tolerant error correction

There are exceptions to the common paradigm, sketched in Figure 1, of alternating computational and error correction steps. In a scheme proposed by Knill, for example, error-correction and computation are performed simultaneously by teleporting into specially prepared ancilla states [Kni04a]. Zalka [Zal97] has suggested balancing the costs of computation and error correction by having multiple computation steps between error-correction rounds, but error propagation between code blocks makes such a scheme challenging to analyze precisely. Surface-code-based quantum fault-tolerance schemes make a more radical change: they implement encoded gates using gradual code deformation, during which error correction occurs frequently. However, while these schemes appear very promising [RHG06, RH07], they have proved difficult to analyze precisely and rigorously [DKLP02].

A variety of error-correction techniques have been studied, and three broad categories are so-called Shor-type [Sho96], Steane-type [Ste97] and Knill-type [Kni04a] error correction. This is only a rough categorization, and it leaves significant room for introducing new ideas and optimization within or beyond these categories; see, e.g., [Rei04, DA07, AC07]. The Shor-, Steane- and Knill-type error-correction schemes rely on the use of ancillary qubits to extract error information from the data blocks. Before interacting with the data, the ancilla qubits need to be prepared in an entangled state. (Surface-code-based schemes are again an exception, and the nine-qubit Bacon-Shor code is an exception at the first level of code concatenation.)

As a concrete example, consider Steane-type error-correction. Arbitrary errors can be written as linear combinations of tensor products of Pauli errors: the identity  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , a bit-flip error  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ , a phase-flip error  $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ , and both bit- and phase-flip errors  $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = iXZ$ . Each tensor product can itself be decomposed as a product of a  $Z$ -error part—a tensor product of  $I$  and  $Z$  operators—and an  $X$ -error part—a tensor product of  $I$  and  $X$  operators. Steane error-correction works by correcting  $Z$  and  $X$  errors separately. First,  $Z$  errors are copied from the data to an encoded  $|0\rangle$  ancilla by transversal CNOT gates, i.e., CNOT gates from each qubit of the ancilla block to the corresponding qubit of the data.  $X$  errors are similarly copied onto an encoded ancilla state  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ . The ancillas are then measured in order to determine a correction.

Preparing ancilla states can be complicated, particularly because errors in the preparation circuit can spread through the ancilla block. For example, a single physical fault may lead to errors on multiple ancilla qubits. The code is limited by its distance and cannot necessarily protect against such correlated errors. As a result, the ancilla states themselves must be checked for errors.

The complexity of verifying prepared ancillas against errors grows quickly as the code distance increases. For large codes, verification of encoded  $|0\rangle$  and  $|+\rangle$  is accomplished by using additional identically prepared “auxiliary” ancillas. In a manner similar to error correction, errors from the initial ancilla are copied onto the auxiliary ancillas and then the auxiliary ancillas are measured. If measurements imply the presence of an error, then all of the ancillas are discarded and the entire process begins anew. Otherwise, the ancilla is accepted and may be used for error correction. Of course, the auxiliary ancillas may also contain errors. These errors can spread to the initial ancilla and invalidate the verification. Thus the auxiliary ancillas must also be checked for errors by yet more ancillas. The end result is a series of recursive verifications that involves many encoded ancillas, and dominates the overall overhead cost of error correction.

To maximize efficiency, preparation and verification circuits may be constructed using a pipeline architecture in which part of the computer is dedicated to preparing many ancillas in parallel. Even so, ancilla production constitutes the majority of the space requirement for a fault-tolerant quantum circuit. In [IWPk08], for example, the ancilla pipeline is estimated to take up to 68 percent of the entire circuit footprint.

For the Golay code, this recursive verification technique requires twelve encoded ancillas and at least 1177 CNOT gates. One such circuit is shown in Figure 2. Variants of this circuit have been used in previous studies of the Golay code, including in [Ste03] and [CDT09]. The construction of this circuit implicitly assumes a kind of worst-case error behavior in which all possible codeword preparation circuits propagate errors in the same way. However, DiVincenzo and Aliferis [DA07] have observed that different preparation circuits exhibit different error propagation behavior, and this can be exploited. By considering many different preparation circuits, we observe that some circuits give favorable combinations of correlated errors, and thus require fewer error verification steps, substantially reducing overhead. In Section 3 we provide two circuits that require only four

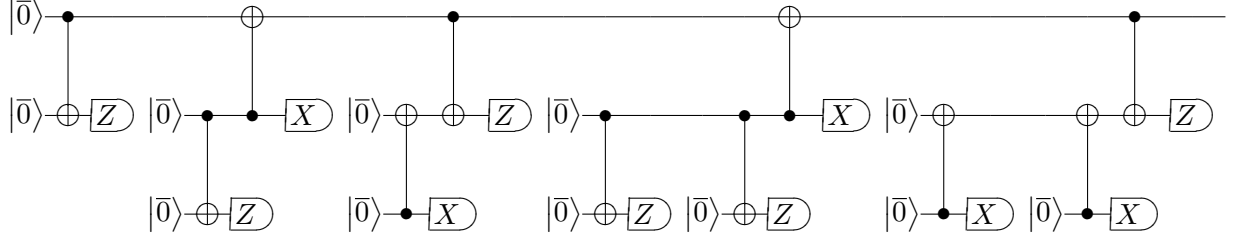


Figure 2: This circuit produces a single Golay encoded  $|0\rangle$  state that is ready to be used in fault-tolerant error correction. Each of the twelve encoded  $|0\rangle$  ancillas, denoted  $|\bar{0}\rangle$ , is identically prepared using the Steane Latin rectangle method (see [Section 3.1](#)). The wires represent 23-qubit code blocks and the indicated CNOT and measurement operations are transversal.

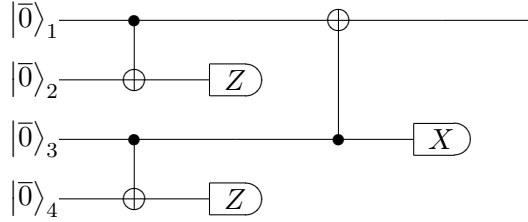


Figure 3: Our simplified ancilla preparation and verification circuit uses only four encoded  $|0\rangle$  ancillas. The ancillas are prepared using different encoding circuits, shown in [Figure 4](#) and [Table 1](#).

encoded  $|0\rangle$  ancillas and as few as 297 CNOT gates. One of these circuits is specified by [Figures 3](#) and [4](#), and [Table 1](#).

The overhead required to prepare a fault-tolerant ancilla depends on the probability that any errors are detected. [Table 2](#) shows estimates of the probability that all of the verification stages accept along with the corresponding expected resource requirements for the different verification circuits. For depolarizing noise rates near  $p = 10^{-3}$ , our circuits reduce both the expected number of qubits and the expected number of CNOT gates by roughly a factor of four over the twelve-ancilla circuit. A more detailed analysis of the acceptance probability and overhead is given in [Section 4.2](#).

## 1.2 Code concatenation and the noise threshold

We consider fault-tolerant, noisy simulations constructed by compiling an ideal quantum circuit into a sequence of *rectangles*, each of which contains an encoded operation and a trailing error correction (TEC). Following [\[AGP06\]](#), we define a rectangle to be *correct* if the action of the rectangle followed by an ideal decoder, i.e., a decoder containing no errors, is equivalent to the action of an ideal decoder followed by an ideal implementation of the corresponding gate. If a rectangle is not correct then it is *incorrect*. In other words, a correct rectangle effectively acts as an encoded version of the intended gate. If all rectangles are correct then a simple induction argument shows that the compiled, noisy circuit successfully simulates the original ideal circuit.

For a fixed stochastic noise model and a fixed quantum error-correcting code, the probability that a rectangle is correct is a constant and therefore the probability that all rectangles are correct will generally be exponentially small in the number of gates in the circuit being simulated. To achieve a constant success probability, a process known as code concatenation [\[KL96\]](#) is often used. In a concatenated fault tolerant simulation, each gate is first compiled into a rectangle, called a

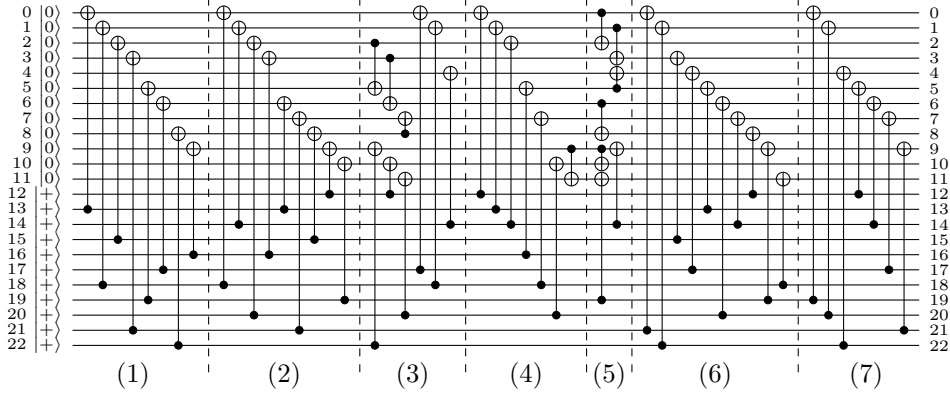


Figure 4: An optimized circuit for preparing  $|0\rangle$  encoded in the Golay code uses 57 CNOT gates applied in seven rounds. Gates in the same round are applied in parallel. The construction is detailed in [Section 3.2](#).

Ancilla	Qubit permutation
$ \bar{0}\rangle_2$	(20, 0, 11, 19, 8, 4, 15, 12, 22, 18, 16, 2, 14, 7, 1, 10, 9, 3, 21, 5, 13, 17, 6)
$ \bar{0}\rangle_3$	(14, 10, 11, 13, 15, 7, 12, 3, 19, 20, 8, 22, 16, 18, 6, 1, 2, 21, 4, 0, 5, 9, 17)
$ \bar{0}\rangle_4$	(12, 0, 10, 11, 17, 3, 1, 19, 8, 6, 18, 20, 4, 2, 14, 7, 13, 9, 22, 5, 15, 16, 21)

Table 1: The first ancilla in [Figure 3](#) is prepared using the circuit of [Figure 4](#). The other three ancillas are prepared in the same way, except with the qubits rearranged according to the above permutations.

Verification	Pr[accept]	E[# qubits]	min # CNOTs	E[# CNOTs]
Steane-12	$0.419 \pm 0.001$	$5183 \pm 14.2$	1177	$1782 \pm 4.9$
Steane-4	$0.648 \pm 0.002$	$1413 \pm 3.7$	377	$497.6 \pm 1.3$
Overlap-4	$0.633 \pm 0.002$	$1399 \pm 3.8$	297	$399.4 \pm 1.1$

Table 2: Estimates of the acceptance probability and overhead for the twelve-ancilla fault-tolerant ancilla preparation circuit and our two optimized circuits, at a depolarizing noise rate of  $p = 10^{-3}$ . The Steane-4 circuit is based on ancillas prepared according to [Table 4](#). Overlap-4 is based on ancillas prepared according to [Figure 4](#) and [Table 1](#). The column labeled Pr[accept] gives the probability that all auxiliary ancilla measurements in the verification circuit detect no errors. The next column, E[qubits], gives the expected number of physical qubits required to produce one verified encoded  $|0\rangle$ . This is calculated recursively, by computing the expected number of qubits needed to pass each verification step. The last two columns specify, respectively, the minimum number of CNOT gates and the expected number of CNOT gates required to produce a single verified ancilla.

level-one rectangle (1-Rec), as described above. Then, a level-two rectangle (2-Rec) is constructed by compiling each physical gate of the 1-Rec into a rectangle. This process is repeated as many times as desired. The end result is a circuit composed of a hierarchy of rectangles.

At each level  $k$  of concatenation, the probability that the  $k$ -Rec is correct increases relative to level  $k - 1$  so long as the strength of the noise is below a certain value called the *threshold*. The threshold is calculated by upper bounding the probability that each type of rectangle is incorrect. In [AGP06] the upper bound is obtained by counting *malignant* sets of locations inside an object called the *extended rectangle*, or exRec, which consists of the rectangle together with its leading error correction (LEC). A set of locations is considered malignant if there exists some fixed combination of nontrivial Pauli errors acting on that set of locations that causes the rectangle to be incorrect.

Malignant set counting works for a broad class of noise models including so-called adversarial noise in which locations fail independently at random, but the error at each failing location is chosen by an adversary and may be correlated with errors at other failing locations. For more restricted noise models such as depolarizing noise, however, malignant set counting is overly pessimistic. Roughly, this is because the definition of a malignant set is independent of the underlying noise model and, therefore, a large amount of information is ignored.

In Sections 4.3 and 4.4 we outline a modified malignant set counting technique that more accurately computes the threshold for depolarizing noise acting on fault-tolerant simulations constructed with our error-correction circuits. Our counting method introduces two new ideas. First, for computational efficiency, we break up the exRec into a hierarchy of components and count  $X$  and  $Z$  errors separately to keep the total number of error combinations small. This technique allows us to analyze larger subsets of faulty locations than would otherwise be possible. Second, we construct at each level a transformed noise model, similar to depolarizing noise, by separately accounting for multiple types of malignant events. ExRecs at each level of code concatenation behave in a self-similar manner under the transformed noise, thus admitting a straightforward threshold calculation.

## 2 The Golay code

The Golay code is a perfect CSS  $[[23, 1, 7]]$  quantum error-correcting code (see e.g., [Ste03]). It has eleven  $X$  and eleven  $Z$  stabilizer generators. The code is self-dual, and the  $X$  and  $Z$  stabilizer generators can both be given by the following eleven 23-character strings:

$$\begin{aligned}
& . 1 . . 1 . . 1 1 1 1 1 . . . . . 1 \\
& 1 . . 1 . . 1 1 1 1 1 . . . . . 1 . \\
& . 1 1 . 1 1 1 . . . 1 1 . . . . . 1 . . \\
& 1 1 . 1 1 1 . . . 1 1 . . . . . 1 . . . \\
& 1 1 1 1 . . . 1 . . 1 1 . . . . . 1 . . . \\
& 1 . 1 . 1 . 1 1 1 . . 1 . . . . . 1 . . . . \\
& . . . 1 1 1 1 . 1 1 . 1 . . . . . 1 . . . . . \\
& . . 1 1 1 1 . 1 1 . 1 . . . . . 1 . . . . . \\
& . 1 1 1 1 . 1 1 . 1 . . . . . 1 . . . . . \\
& 1 1 1 1 . 1 1 . 1 . . . . . 1 . . . . . \\
& 1 . 1 . . 1 . . 1 1 1 1 1 . . . . .
\end{aligned} \tag{2.1}$$

Here, the 1s in a row either all indicate  $Z$  operators or all indicate  $X$  operators, and dots indicate identity operators. For example, the first line indicates that  $I \otimes Z \otimes I \otimes I \otimes Z \otimes \cdots \otimes Z$  and  $I \otimes X \otimes I \otimes I \otimes X \otimes \cdots \otimes X$  are stabilizers. Note that each stabilizer generator has weight eight. We index the qubits left to right, from 0 to 22.

The stabilizer generators partition the group of Pauli errors on 23-qubits into  $2^{24}$  cosets. In particular, there are  $2^{23-11} = 2^{12}$  inequivalent  $X$  errors (tensor products of  $X$  and  $I$ ) and  $2^{12}$  inequivalent  $Z$  errors (tensor products of  $Z$  and  $I$ ).

The Golay code is preserved by qubit permutations in a symmetry group known as the Mathieu group  $M_{23}$ . This is a four-transitive group of order  $23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$ . It is generated by a cyclic shift, and by the permutation  $(2, 16, 9, 6, 8)(3, 12, 13, 18, 4)(7, 17, 10, 11, 22)(14, 19, 21, 20, 15)$ , in cycle notation.

### 3 Ancilla preparation and verification

Our error-correction circuits require multiple encoded  $|0\rangle$  and  $|+\rangle$  states. The Golay code is self-dual, so encoded  $|+\rangle$  is prepared by taking the dual of the  $|0\rangle$  circuit in the natural way (i.e., swapping  $|0\rangle$  and  $|+\rangle$  and reversing the direction of each CNOT gate). There are many possible ways to encode  $|0\rangle$ . Our most efficient preparation circuit is shown in Figure 4, and prepares encoded  $|0\rangle$  in the Golay code with a total of 57 CNOT gates. This circuit provides an efficient means of preparing encoded ancillas, but it is not fault-tolerant on its own.

We define strict fault-tolerance as follows:

**Definition 3.1.** *An ancilla encoded into a code with distance  $d$  is strictly fault-tolerant if for all  $k \leq \lfloor d/2 \rfloor$ , any error of probability order  $k$  propagates to an error of weight at most  $k$ .*

The circuit in Figure 4 is clearly not strictly fault-tolerant because, for example, with first order probability a faulty CNOT gate may produce an error of weight two when an  $X$ -error occurs on both its control qubit and its target qubit. We call this error, and any other for which the weight of the resulting error is larger than the probability order with which it occurs, “correlated”.

To achieve strict fault tolerance, additional encoded ancillas are prepared. Errors from the “target” ancilla are copied onto the additional ancillas which are then measured. If no errors are detected, the ancilla is accepted and may be used for error correction on the data. Otherwise, the ancilla is rejected, all of the prepared ancillas are discarded, and the procedure is restarted. In Figure 3, two pairs of ancillas are prepared. One of the ancillas from each pair is checked for  $X$  errors. If neither check detects an error, then one of the two remaining ancillas is used to check the other for  $Z$  errors.

Care must be taken in preparing the additional ancillas, however. For example, say that two encoded ancillas are identically prepared. Assume that a single failure occurs in the first ancilla and propagates through the preparation circuit to produce a weight three error. Then the same single failure in the other ancilla will produce the *same* weight three error. When the error from the first ancilla is copied to the second, the two errors will cancel each other and no error will be detected. This is a second order event that results in a weight-three error.

Therefore, we seek to prepare encoded ancillas that produce different correlated error sets. In this section we provide two related methods for constructing fault-tolerant ancillas encoded in the Golay code using the circuit in Figure 3. In Section 3.1 we analyze the correlated errors produced by preparation circuits constructed with the standard Latin rectangle method and provide a randomized



Weight:	0	1	2	3	4	5	6	7
Number of $X$ errors:	1	23	253	1771	1771	253	23	1
Number of $Z$ errors:	1	23	253	1771	0	0	0	0

Table 3: The number of errors on Golay encoded  $|0\rangle$  by Hamming weight. All  $Z$  errors are correctable so there are no  $Z$  errors of weight greater than three.

method for finding ancillas with different correlated error sets. In [Section 3.2](#) we describe a new preparation circuit specific to the Golay code and again provide a randomized method for finding ancillas with different correlated error sets.

### 3.1 Randomized method for preparing encoded $|0\rangle$

The standard method for preparing encoded states for CSS stabilizer codes, including the Golay code, is to construct and solve a partial Latin rectangle based on the stabilizer generators [Ste02]. To prepare  $|0\rangle$  in the Golay code, consider the eleven stabilizer generators that are tensor products of Pauli  $X$  operators. These stabilizer generators form an  $11 \times 23$  binary matrix in which the  $X$  operators in the tensor product are represented as 1s, as in Eq. (2.1). Gaussian elimination is performed until the matrix is of the form

$${}_{11} \left\{ \left( \begin{array}{c|c} \overbrace{I}^{11} & \overbrace{A}^{12} \end{array} \right) \right. \quad (3.1)$$

The first eleven qubits, called “control” qubits, are prepared as  $|+\rangle$ , and the remaining “target” qubits are prepared as  $|0\rangle$ . The matrix  $A$  represents a partial Latin rectangle, the solution to which is used to schedule rounds of CNOT gates from control to target qubits.

An  $X$  error in the preparation circuit can propagate to other qubits only if it occurs on a control qubit, and then only through the  $X$  stabilizer being created from that control qubit. Thus single faults can create up to 22 weight-two errors (for each of the eleven  $X$  stabilizers, either  $IIIIIIIXX$  or  $IIXXXXXX \sim XXIIIIII$ ), 22 weight-three errors and eleven weight-four errors ( $IIIIXXXXX$  for each stabilizer).

A single  $X$  fault, i.e., a fault resulting in an  $X$  error, cannot break the verification circuit in [Figure 3](#). If it creates a correlated error on the first ancilla, that error will be detected on the second ancilla, and both will be discarded. Four or more  $X$  faults also cannot break our the verification circuit because we only seek fault tolerance up to order three.

Two  $X$  faults can break the verification circuit only if there is one failure in each ancilla preparation that propagates to an error of weight at least three—necessarily the same error so that it is undetected. To obtain a crude estimate for how likely this is to occur, pretend that the correlated errors created by a random preparation circuit are uniformly distributed among all errors of the same weights. The number of errors on encoded  $|0\rangle$  for each weight are given in [Table 3](#). Then the probability that two preparation circuits share no such correlated errors is estimated as

$$\frac{\binom{1771-22}{22}}{\binom{1771}{22}} \cdot \frac{\binom{1771-11}{11}}{\binom{1771}{11}} \approx 0.71 \quad .$$

Three  $X$  errors can break the circuit if they lead to an undetected error of weight four or greater on the first ancilla. Consider the case that there are two failures while preparing the first ancilla and one failure while preparing the second ancilla. The number of different weight-four errors created



	1	2	3	4	5	6	7		1	2	3	4	5	6	7		1	2	3	4	5	6	7		1	2	3	4	5	6	7
2	0	22	7	11	4	8	19	0	5	16	17	22	1	15	9	1	21	16	7	13	10	15	0	0	1	16	3	12	17	13	11
3	9	19	4	8	7	1	6	3	15	2	6	5	17	16	11	2	16	7	12	0	18	19	13	2	22	18	14	3	20	17	6
10	5	1	0	6	14	7	9	7	1	22	4	17	2	5	6	3	13	0	15	12	19	10	20	4	3	20	6	1	12	22	13
12	1	0	14	5	22	11	4	8	6	13	16	1	15	4	17	4	12	21	18	20	7	13	10	5	6	14	16	20	1	12	17
13	6	8	22	9	0	4	5	10	22	11	5	13	16	6	1	5	6	13	21	10	0	18	19	7	20	22	17	13	16	18	1
15	4	5	9	14	19	22	7	12	9	17	13	2	6	22	16	8	18	19	13	21	15	20	16	8	16	6	18	11	3	1	20
16	14	7	5	4	11	6	8	14	4	6	11	15	13	2	22	9	19	6	10	15	20	7	21	9	18	12	13	16	14	20	3
17	8	11	6	19	5	0	1	18	16	1	15	11	9	13	2	11	20	12	6	7	13	16	15	10	14	17	20	22	13	11	12
18	7	9	1	22	8	5	11	19	17	4	1	9	22	11	13	14	7	18	20	16	21	0	6	15	12	11	1	17	18	6	22
20	19	6	11	7	1	14	22	20	11	15	9	6	4	1	5	17	0	15	19	6	16	21	12	19	17	13	11	18	6	16	14
21	11	4	19	0	6	9	14	21	2	5	22	16	11	9	4	22	10	20	16	19	6	12	18	21	11	3	12	6	22	14	16

(a) Ancilla 1                      (b) Ancilla 2                      (c) Ancilla 3                      (d) Ancilla 4

Table 4: Four seven-round ancilla-preparation schedules. In each table, the entry in row  $i$ , column  $j$  specifies the target qubit of a CNOT gate with control qubit  $i$  applied in round  $j$ . Using these schedules in the verification circuit of Figure 3, the output encoded  $|0\rangle$  state is fully fault-tolerant against both  $X$  and  $Z$  errors.

with second-order probability (i.e., excluding those created with first-order probability) depends on the circuit. For ten random circuits, the smallest count we obtained was 688 and the largest 735, with an average of 711. Using this average value, we estimate that the probability of a random circuit succeeding against three  $X$  errors is roughly  $[(\binom{1771-711}{11}) / (\binom{1771}{11})]^2 \approx 1.2 \cdot 10^{-5}$ . (Here the square is because we want the circuit to work against both the case of two failures in the first ancilla, one failure in the second, and vice-versa.) Overall, we expect to have to try about  $1.2 \cdot 10^5$  random pairs of preparation circuits before we find one that gives fully fault-tolerant  $X$ -error verification.

The result of  $X$ -error verification is a single ancilla free of correlated  $X$  errors up to weight-three, but possibly containing correlated  $Z$  errors. The  $Z$ -error propagation can be analyzed in a manner similar to that used for  $X$  errors. A single failure in an  $X$ -error verified ancilla can produce roughly 60  $Z$  errors of weight three. Again assuming a uniform distribution, the probability of finding two  $X$ -error verified ancillas that share no correlated  $Z$  errors of weight three is  $(\binom{1771-60}{60}) / (\binom{1771}{60}) \approx 0.12$ . In total, we expect to try about five  $X$ -error fault-tolerant pairs in order to find two pairs that are fully fault-tolerant for both  $X$ -error and  $Z$ -error verification, as  $\binom{5}{2} = 10$ .

To find fault-tolerant verification circuits in this way, one needs to be able to generate sufficiently random preparation circuits. As the Latin rectangle procedure for finding encoding circuits is fully algorithmic, it can be randomized by starting with a random presentation of the Golay code. Alternatively, one can begin with a fixed encoding circuit and randomly permute the seven rounds of CNOT gates (all of the CNOTs commute), or permute the qubits according to a random element of the symmetry group  $M_{23}$ . By trying roughly  $10^5$  random pairs, we found 14 pairs of ancillas that were fully fault-tolerant against  $X$  errors. Of the  $\binom{14}{2}$  combinations, six were also fully fault-tolerant against  $Z$  errors. Table 4 presents one such set.

### 3.2 Overlap method for preparing encoded $|0\rangle$

The above procedure for finding a fault-tolerant verification circuit uses ancilla preparation circuits constructed from the Latin rectangle method. We now show an alternative construction based on a modification of the Latin rectangle method. By carefully analyzing the stabilizer generators of the Golay code we can reduce the number of CNOT gates required to prepare encoded  $|0\rangle$ .

To explain the optimization, first consider the Steane  $[[7, 1, 3]]$  code. A Latin rectangle-based encoding schedule, shown in Figure 5(a), needs nine CNOT gates. An equivalent circuit requiring

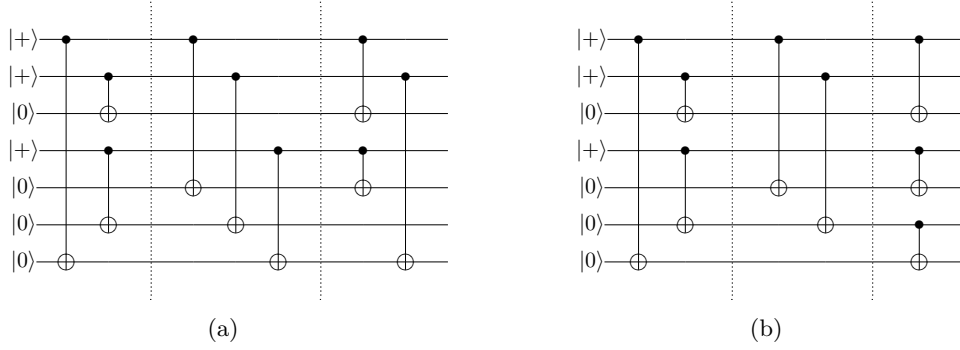


Figure 5: Two alternative circuits for preparing encoded  $|0\rangle$  in the Steane code, a self-dual code with  $X$  stabilizers  $IIIXXXX$ ,  $IXXIIIX$  and  $XIXIXIX$ . The circuit in (a) follows Steane’s Latin rectangle encoding method. The circuit in (b) prepares the same state using one fewer CNOT gate. The new CNOT gate has the same effect as the two removed gates.

$X$ -error weight:	2	3	4	5	6	7
Order 1:	16	14	4	0	0	0
Order 2:	-	493	400	35	2	0

Table 5: Correlated  $X$ -error counts for the encoded  $|0\rangle$  circuit in Figure 4.

only eight CNOT gates is shown in Figure 5(b). This circuit removes two of the CNOTs for which qubit six is a target and replaces them with a single CNOT from qubit five to qubit six in round three. This works because in 5(a) qubits five and six are both the targets of CNOTs from qubits one and three; the corresponding stabilizer generators overlap on qubits five and six.

The same technique of exploiting overlap between stabilizers extends to larger CSS codes. For the Golay code, Figure 4 gives an encoding circuit with only 57 CNOT gates, 20 fewer than given by the Latin rectangle method.

By reducing the number of CNOT gates, this circuit also reduces the number of correlated errors. For example, a single failure in the Latin rectangle encoded circuits can cause up to 22 weight-two errors, but a single failure in the new circuit can only cause up to 16 weight-two errors. The correlated error counts for first and second order are shown in Table 5. The smaller number of correlated errors means that it should be easier to find fault-tolerant circuits by randomization. However, unlike Steane schedules the overlap schedule depends on a fixed code presentation and on a fixed round ordering, since the CNOT gates do not commute.

To obtain randomized overlap method encoding circuits, we use the permutation symmetry of the Golay code and permute the qubits of Figure 4 according to a pseudo-random element of the symmetry group  $M_{23}$ . By analyzing the correlated error sets of randomly permuted circuits, we have found many sets of fault-tolerant four-ancilla preparation circuits. In fact, we have even found sets for which the order required for a weight- $k$  error to pass verification is at least  $k + 1$  (rather than  $k$ ) for all  $k \leq 2$ . This reduces, for example, the probability of accumulating an uncorrectable error on the data block by first a weight-two error in  $Z$ -error correction and then another weight-two error in  $X$ -error correction. One such set of four permutations is given in Table 1.

## 4 Overhead and threshold analysis

The remainder of this article focuses on analyzing the overhead and noise threshold for fault-tolerant quantum computation using the Golay code ancilla preparation and verification circuits from [Section 3](#). Our overhead analysis, in [Section 4.2](#), is based on Monte Carlo computer simulations with a depolarizing noise model. Our threshold analysis relies on a malignant set counting technique that is tailored for the same depolarizing noise model. The counting technique is outlined in [Section 4.3](#) and proof of the threshold lower bound is presented in [Section 4.4](#). (Some details are given in the appendices.) Threshold calculation results for our circuits are discussed in [Section 4.5](#).

### 4.1 Noise model

We begin by defining the depolarizing noise model, a standard model used before in, e.g., [\[Kni04b\]](#). We study noisy circuits constructed from the following physical operations:  $|0\rangle$  and  $|+\rangle$  initialization, a CNOT gate, and single-qubit measurement in the  $Z$  and  $X$  eigenbases. Every qubit in the computer can be involved in at most one operation per discrete time step. CNOT gates are allowed between arbitrary qubits, without geometry constraints. Resting qubits are also subject to noise.

**Definition 4.1** (Independent depolarizing noise with parameter  $\gamma$ ). *Noisy operations are modeled by:*

1. *A noisy CNOT gate is a perfect CNOT gate followed by, with probability  $\frac{16}{15}\gamma$ , the simultaneous depolarization of the two involved qubits. Equivalently, after applying the ideal CNOT gate, with probability  $15\gamma$  a non-trivial two-qubit Pauli error drawn uniformly and independently from  $\{I, X, Y, Z\}^{\otimes 2} \setminus \{I \otimes I\}$  is applied.*
2. *Noisy preparation of a  $|0\rangle$  state is modeled as ideal preparation of  $|0\rangle$ , followed by application of an  $X$  error with probability  $4\gamma$ . Similarly, noisy preparation of  $|+\rangle$  is modeled as ideal preparation of  $|+\rangle$  with probability  $1 - 4\gamma$  and of  $|-\rangle = Z|+\rangle$  with probability  $4\gamma$ .*
3. *Noisy  $Z$ -basis ( $|0\rangle, |1\rangle$ ) measurement is modeled by applying an  $X$  error with probability  $4\gamma$ , followed by ideal  $Z$ -basis measurement. Similarly, noisy  $X$ -basis ( $|+\rangle, |-\rangle$ ) measurement is modeled as ideal measurement except preceded by a  $Z$  error with probability  $4\gamma$ .*
4. *A noisy rest operation is modeled as applying either the identity gate, with probability  $1 - 12\gamma$ , or with probability  $4\gamma$  each, one of the Pauli errors  $X$ ,  $Y$  or  $Z$ .*

*All locations fail independently of each other. Let  $p = 15\gamma$ , the probability for a CNOT gate to fail.*

To justify this noise model, note that the noise on a resting qubit is the one-qubit marginal of the CNOT gate noise. The noise rate for preparation and measurement is lower, only  $4\gamma$ , because any higher noise rate could be reduced to  $4\gamma + O(\gamma^2)$  by repeating the preparation or measurement operation using two qubits coupled by a CNOT.

During error counting,  $X$  and  $Z$  errors are usually considered separately and the error probability is computed by omitting the  $Z$  or  $X$  part of each error, respectively. For example, when considering only  $X$  errors  $XY$  is equivalent to  $XX$ ,  $XZ$  is equivalent to  $XI$  and so on. Thus, the marginal distribution of  $X$  errors for a CNOT gate applies with probability  $12\gamma$  a uniformly random error from  $\{IX, XI, XX\}$ . Similarly, for  $Z$  errors, the marginal error distribution applies a random error from  $\{IZ, ZI, ZZ\}$ . For preparing  $|0\rangle$  or measuring in the  $Z$  basis, no  $Z$  errors are possible, and similarly no  $X$  errors are possible for preparing  $|+\rangle$  or measuring in the  $X$  basis. The marginal  $X$ - and  $Z$ -error distributions for a rest are to apply  $X$  or  $Z$  errors with probability  $8\gamma$ .

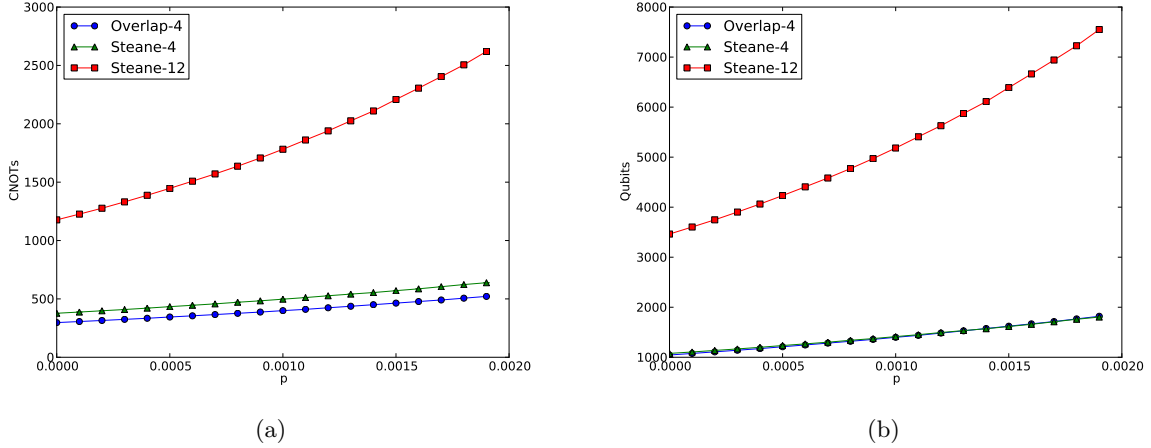


Figure 6: Overhead for the twelve-ancilla ancilla preparation and verification circuit and for each of our optimized circuits. (a) Expected number of CNOT gates required to produce a verified encoded  $|0\rangle$ . (b) Number of qubits required to produce one verified encoded  $|0\rangle$ , in expectation, at every time step. Standard error intervals are too small to be seen here.

## 4.2 Simulation of the overhead

To evaluate the practical importance of our optimizations, we now analyze the resource requirements of our ancilla preparation and verification circuits. One natural measure for this overhead is the number of CNOT gates used to ready an ancilla. Another overhead measure, important given the difficulty of scaling quantum computers, is the space complexity, i.e., the number of qubits that must be dedicated to ancilla preparation in a pipeline so that an ancilla is always ready in time for error correction. We consider both measures.

As listed in the third column of Table 2, the overlap method-based four-ancilla preparation and verification circuit involves roughly a factor of four fewer CNOT gates than the standard twelve-ancilla circuit. In fact, this understates the improvement. The overhead also depends on the acceptance rates of each verification test. For an ancilla to leave the twelve-ancilla circuit, it must pass eleven tests, compared to only three tests for the four-ancilla circuit. The probability of passing all tests should be significantly higher for the optimized circuit, and so one expects the ratio between the *expected* numbers of CNOT gates used by the two circuits to be greater than four.

To estimate the expected overhead, each circuit was modeled and subjected to depolarizing noise in a Monte Carlo computer simulation. We assumed that test results are available soon enough that a failed verification circuit can be immediately aborted; later test failures are therefore the most costly. This assumption impacts the twelve-ancilla circuits the most, since there are many ways to construct the hierarchy of verifications. The circuit shown in Figure 2 is a reasonable choice here because only six of the verification tests depend on results of previous tests. Other circuits may contain as many as nine dependent tests.

Estimates of the expected number of CNOT gates required for each circuit are given in the last column of Table 2 for CNOT depolarization rate  $p = 10^{-3}$ , and are plotted versus  $p$  in Figure 6(a). At  $p = 10^{-3}$ , the overlap method reduces the expected number of CNOT gates by roughly a factor of 4.5, compared to the twelve-ancilla circuit, and the improvement for our optimized Latin rectangle

scheme is a factor of about 3.6. At lower error rates, the improvement is less. To investigate the effects of different error parameters, we also considered setting the rest error rate to zero; in this case, the expected number of CNOT gates used in the overlap circuit further decreases by about 11 percent, compared to less than four percent for our other four-ancilla circuit and less than two percent for the twelve-ancilla circuit. The larger improvement for the overlap circuit is due primarily to the fact that the overlap preparation method replaces many CNOT gates with rest locations.

To evaluate the space overhead, we plot in [Figure 6\(b\)](#) the number of qubits required to produce a single verified encoded  $|0\rangle$ , in expectation, per time step, for each of the preparation and verification circuits. Thus, for example, the space overhead for a pipeline to produce a single *unverified* ancilla state is  $8 \cdot 23 = 184$  qubits; at any given time step, one 23-qubit block is initialized, and CNOT gates are applied to seven other blocks—one per round in, e.g., [Figure 4](#)—so that one ancilla is prepared. (In fact, the overhead is slightly less than this since some of the qubits in the block can be prepared during rounds one and two.) Estimates are calculated recursively by computing  $E[\text{qubits}] = (E[\text{qubits}]_1 + E[\text{qubits}]_2) / \text{Pr}[\text{accept}]$  for each verification step where the numerator is the expected number of qubits required to prepare the two states used in that verification step and  $\text{Pr}[\text{accept}]$  is the probability that the verification measurement detects no errors. The results at  $p = 10^{-3}$  are given in the second column of [Table 2](#). Both of our optimized schemes reduce the required space by a factor of roughly 3.6 at  $p = 10^{-3}$ .

To judge the significance of these results, we remark again that the ancilla production pipeline can consume the majority of resources in a fault-tolerant quantum computer. In the case of [\[IWPK08\]](#), physical ancilla production space is proportional to the number of CNOT gates in the pipeline. A factor of 4.5 reduction in the CNOT overhead for ancilla preparation should give, very roughly, about a 50 percent improvement in the total footprint of the quantum computer.

### 4.3 Counting malignant sets

As we have shown, our two optimized ancilla preparation and verification circuits significantly reduce the overhead required for fault-tolerant ancilla preparation. We would also like to know how these circuits impact the tolerable noise threshold. With fewer verification stages our ancillas are slightly more likely to contain errors and so one might expect a lower noise threshold when compared to previous verification circuits. On the other hand, the smaller size of our circuits makes it easier to give a tighter analysis.

The threshold calculation is most limited by the exRec with the largest number of locations. The Golay code admits transversal implementations of encoded Clifford group unitaries. Universality can be achieved by injection and distillation [\[BK05, Kni04b\]](#), which involves only Clifford group unitaries, and the single-qubit preparations and measurements that are already assumed by our model. Therefore the largest exRec in our case is for the encoded CNOT gate, an exRec that consists of four Steane-type error corrections plus 23 CNOT gates (see [Figure 7](#)). [Table 6](#) gives a breakdown of the number of locations for our preparation circuits, and the total number of locations in the CNOT exRec.

Monte Carlo simulations of circuits using the Golay code [\[Ste03, CDT09\]](#) indicate that the depolarizing noise threshold should be on the order of  $p = 10^{-3}$ . Unfortunately, it is not straightforward to prove such a high threshold using malignant set counting. For example, say that we check for malignancy all location subsets of size up to  $k_{\text{good}}$ , and we assume that all larger subsets are malignant. Then the estimate we obtain for the probability of an incorrect rectangle is at least  $\sum_{k=k_{\text{good}}+1}^n \binom{n}{k} p^k (1-p)^{n-k}$ . For  $n = 5439$  locations and  $p = 10^{-3}$ , this term drops below  $10^{-3}$

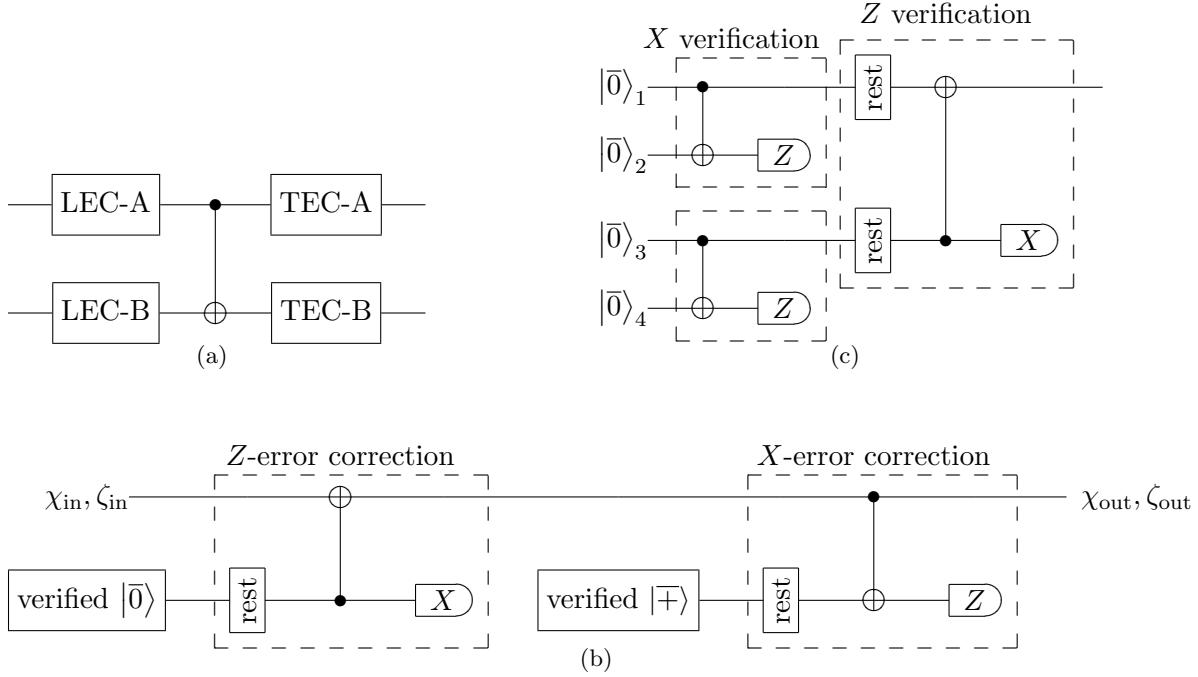


Figure 7: Organization of a CNOT extended rectangle, or “exRec.” (a) The CNOT exRec includes four error corrections, two leading (LEC) and two trailing (TEC), and a transversal CNOT gate. (b) Each error-correction component consists of separate Z and X error corrections. Z-error correction requires a  $|\bar{0}\rangle$  state that has been verified against errors, and X-error correction requires a verified  $|\bar{+}\rangle$  ancilla state. (c) A verified  $|\bar{0}\rangle$  state is prepared by checking two pairs of prepared  $|\bar{0}\rangle$  states against each other for X errors, then, conditioned on no X errors being detected, checking the results against each other for Z errors. Verified  $|\bar{+}\rangle$  is prepared by taking the dual of the  $|\bar{0}\rangle$  circuit. These components are discussed, in reverse order, in Sections 4.3.2 to 4.3.5.

only for  $k_{\text{good}} \geq 14$ . However, there are more than  $10^{41}$  subsets of size at most 14, so checking them one at a time is computationally intractable.

Instead of checking each set for malignancy, one can sample random sets of locations in order to estimate the fraction that are malignant. This technique, called malignant set sampling, can provide threshold estimates with statistical confidence intervals. However, both malignant set counting and sampling techniques study the threshold for worst-case adversarial noise, and may be overly conservative for a more physically realistic, non-adversarial noise model such as depolarizing noise. For example, malignant set sampling results from [AC07] estimate a threshold of only  $p \approx 10^{-4}$  for the Golay code.

We therefore present an alternative to malignant set counting that is tailored to circuits based on the Golay code and depolarizing noise. Roughly, we divide the exRec into a hierarchy of components and sub-components. We then compute an upper bound on the probability of each error a component may produce, essentially by checking location sets up to a certain small size. At the exRec level, we synthesize the component error bounds into upper bounds on the probability that the rectangle is incorrect. The resulting error probabilities are treated as an effective transformed noise model for the encoded circuit. With some care, the transformed noise model can be fed recursively back into the procedure to determine an effective noise model for the next level of encoding, and so on.

$ \bar{0}\rangle$ preparation circuit	Location type				Total	CNOT exRec total
	CNOT	Prep.	Meas.	Rest		
Steane	77	23	0	6	106	5439
Overlap	57	23	0	38	118	5823

Table 6: Location counts for preparing encoded  $|0\rangle$  in the Golay code. Encoded  $|0\rangle$  ancillas are prepared with either the pseudorandomly constructed Steane preparation circuits (Table 4), or the overlap preparation circuits (Figure 4 and Table 1). The last column shows the total number of locations inside the CNOT exRec shown in Figure 7, including the transversal CNOT operation and four error corrections.

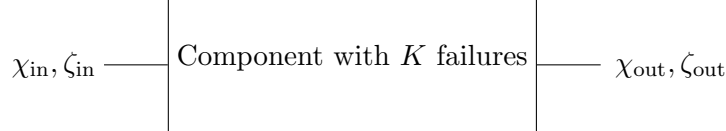


Figure 8: A circuit component with input error  $(\chi_{\text{in}}, \zeta_{\text{in}})$  and output error  $(\chi_{\text{out}}, \zeta_{\text{out}})$

Effectively, dividing the exRec into components allows us to efficiently account for even very large location subsets. Most large sets will be roughly evenly divided, with only a small number of locations in each component.

The remainder of this section outlines our modified malignant set counting technique. Details of the threshold analysis are given in Section 4.4.

#### 4.3.1 Characterizing exRec components

We will divide the exRec into its encoded operation and its error corrections. The error corrections will each divide into  $X$ -error correction and  $Z$ -error correction, and further recursive divisions will continue until reaching the physical location level.

Each component in the hierarchy has input error  $(\chi_{\text{in}}, \zeta_{\text{in}})$ , some number of internal failures  $K$ , and output error  $(\chi_{\text{out}}, \zeta_{\text{out}})$  which depends on the internal failures and on the input error (see Figure 8). For every error equivalence class on the inputs and outputs and for every  $k \in \mathbb{N}$ , we would like to compute

$$\Pr [(\chi_{\text{out}}, \zeta_{\text{out}}) = (x_{\text{out}}, z_{\text{out}}), K = k \mid (\chi_{\text{in}}, \zeta_{\text{in}}) = (x_{\text{in}}, z_{\text{in}})] , \quad (4.1)$$

the probability that there are exactly  $k$  failures and the output error is  $(x_{\text{out}}, z_{\text{out}})$  conditioned on the input error  $(x_{\text{in}}, z_{\text{in}})$ . Here, the notation  $(x, z)$  indicates an error equal to the product  $xz$  where  $x$  is a tensor product of  $X$  and  $I$  operators and  $z$  is a tensor product of  $Z$  and  $I$  operators.

For components that are physical gate locations the probability in (4.1) is defined by the depolarizing noise model (Definition 4.1). Larger components are analyzed by first analyzing each enclosed sub-component. At the exRec level the LEC, transversal CNOT and TEC components provide all of the information necessary to determine the probability that the exRec is incorrect. Indeed, we shall see in Section 4.3.5 that they contain enough information to compute the probability for each *way* that the exRec can be incorrect.

There are, however, two logistical problems. First, on each 23-qubit code block, there are  $2^{12}$  inequivalent  $X$  errors and  $2^{12}$  inequivalent  $Z$  errors, and thus  $2^{24}$  inequivalent Pauli errors total. (For example, there are  $2^{23}$  different tensor products of  $X$  and  $I$  operators, and the group of  $X$



stabilizers has size  $2^{11}$ , leaving  $2^{12}$   $X$ -error equivalence classes.) For a component involving two code blocks, this means we should compute for each  $k$  up to  $(2^{24})^4$  quantities, one for each combination of input and output errors. Second, since there are  $\binom{n}{k}$  size- $k$  subsets of  $n$  locations and since each CNOT gate has 15 different ways to fail, a computation that accounts for all possibilities scales roughly as  $\binom{n}{k} 15^k$ . Such a computation is feasible only for small  $k$  and small  $n$ .

The first problem can be solved by observing that in Steane error correction  $X$  errors and  $Z$  errors are corrected separately. Furthermore, there are no Hadamard gates or other ways of transforming an  $X$  error into a  $Z$  error, or vice versa, so  $X$  and  $Z$  errors mostly propagate independently.  $X$  and  $Z$  errors cannot be treated independently entirely, because  $X$  and  $Z$  failures are highly correlated in the depolarizing noise model, and the postselection steps in ancilla verification could amplify any initial dependencies. Still, for most components, the  $X$ -error part of the output of a component depends only on the  $X$ -error part of the input and the  $X$  failures that occur inside the component. A similar observation holds for  $Z$  errors. Thus, expression (4.1) may be split into separate  $X$  and  $Z$  parts:

$$\Pr[\chi_{\text{out}} = x_{\text{out}}, K_X = k | \chi_{\text{in}} = x_{\text{in}}] \quad (4.2a)$$

$$\Pr[\zeta_{\text{out}} = z_{\text{out}}, K_Z = k | \zeta_{\text{in}} = z_{\text{in}}] \quad (4.2b)$$

Here, the random variable  $K_X$  is the number of failures inside the component that contain an  $X$  when decomposed into a tensor product of Pauli operators. The value  $K_Z$  is similarly defined for  $Z$ . When considering  $X$  and  $Z$  errors separately, the input and output of a two-block component contain at most  $2^{24}$  inequivalent errors and the worst case combination is a large but manageable  $2^{48}$  cases.

The second problem is eliminated by noting that, for a fixed  $k$ , the probability of an order- $k$  fault decreases rapidly as the size of the component decreases. For example, for  $p = 1 \times 10^{-3}$ , the probability of an order-ten fault in the exRec is about 0.027. However, the probability that all ten failures are located in a single error correction is only about  $1.4 \times 10^{-6}$ . Thus there is little gain in counting errors of order-ten or higher in the error correction component.

In general, the probability that a component contains a fault of order greater than  $k_{\text{good}}$  can be bounded according to

$$\Pr[K > k_{\text{good}}] \leq \sum_{k=k_{\text{good}}+1}^n \binom{n}{k} (1-p)^{n-k} p^k \quad (4.3)$$

(A tighter bound can be achieved by considering separate  $k$  for each location type. See [Appendix A.1](#).) We will choose a value of  $k_{\text{good}}$  for each component and then pessimistically assume that all faults of order greater than  $k_{\text{good}}$  within the component cause the rectangle to be incorrect. For large enough values of  $k_{\text{good}}$  the overall impact on the threshold is negligible. There is a tradeoff here between running time and accuracy. A larger value of  $k_{\text{good}}$  yields a more accurate bound on the probability that the rectangle is incorrect. A smaller value of  $k_{\text{good}}$  is easier to compute. We must choose for each component a suitable  $k_{\text{good}}$  that balances the two.

In the end we are left with two sets of faults for each component, those of order at most  $k_{\text{good}}$  and those of order greater than  $k_{\text{good}}$ . Each fault in the first set is counted to obtain accurate estimates of (4.2a) and (4.2b). When a fault from this set occurs we call it a *good* event. Faults in the second set are not counted and are instead bounded using (4.3) and pessimistically added to the final incorrectness probability bounds for the exRec. When a fault from this set occurs we call

it a *bad* event. The probability that the rectangle is incorrect is then upper-bounded by

$$\Pr[\text{incorrect}] \leq \Pr[\text{incorrect, good}] + \Pr[\text{bad}] .$$

In general, there are four quantities we need to upper bound for each component:

$$\Pr[\chi_{\text{out}} = x_{\text{out}}, K_X = k, \text{good}_X | \chi_{\text{in}}], \Pr[\zeta_{\text{out}} = z_{\text{out}}, K_Z = k, \text{good}_Z | \zeta_{\text{in}}], \Pr[\text{bad}_X], \text{ and } \Pr[\text{bad}_Z] .$$

The event  $\text{good}_X \equiv \neg \text{bad}_X$  occurs when there is a set of  $X$ -error failures in the component that we choose to count. It will usually depend only on  $k_{\text{good}}$  in which case  $\text{good}_X \Leftrightarrow (K_X \leq k_{\text{good}})$ . In some cases  $\text{good}_X$  may depend on a vector  $\vec{k}$  representing the number of  $X$ -error failures across multiple sub-components. The event  $\text{good}_Z \equiv \neg \text{bad}_Z$  is similarly defined for  $Z$ .

In the remainder of this section we outline the procedure for computing the above quantities for each component of the CNOT exRec. A more precise analysis is presented in [Appendix A](#).

### 4.3.2 $X$ -error verification

$X$ -error verification requires two encoded  $|\bar{0}\rangle$  states. The first is verified against the second for  $X$  errors by applying transversal CNOT gates between the two code blocks and then measuring each qubit of the second block in the  $Z$  eigenbasis ( $|0\rangle, |1\rangle$  basis). Conditioned on no  $X$  errors being detected, the first code block is accepted. See [Figure 7\(c\)](#).

Letting  $\text{accept}$  denote the event that no  $X$  errors are detected, we use Bayes's rule

$$\Pr[\text{event} | \text{accept}] = \frac{\Pr[\text{event, accept}]}{\Pr[\text{accept}]} \quad (4.4)$$

to compute the conditional probabilities of different error events. For an event  $\chi$  involving only  $X$  errors, this calculation is straightforward.

However, if the event is a  $Z$  error  $\zeta$ , then the numerator  $\Pr[\zeta = z, \text{accept}]$  is difficult to compute as it mixes  $X$  and  $Z$  errors. The obvious bound,  $\Pr[\zeta = z, \text{accept}] \leq \Pr[\zeta = z]$ , is quite pessimistic because in the depolarizing noise model we expect  $X$  errors to occur with  $Z$  errors roughly half of the time, and so  $X$ -error verification should remove many  $Z$  errors. It is important to obtain an accurate count of  $Z$  errors since they strongly influence the acceptance rate of the upcoming  $Z$ -error verification. Therefore, we also count  $X$  and  $Z$  errors *together* for very low-order faults and apply a correction to the  $Z$ -only counts. Details of the correction are worked out in [Appendix A.2](#).

### 4.3.3 $Z$ -error verification

$Z$ -error verification is similar to  $X$ -error verification. However, as shown in [Figure 7\(c\)](#), we add a pause, i.e., transversal rest operations, to allow the preceding  $X$ -error postselection to complete.

Similar to  $X$ -error verification, all events are now conditioned on the event  $\text{accept}$  of no  $Z$  errors being detected. When considering an  $X$ -error event  $\chi$ , we generally use the pessimistic inequality  $\Pr[\chi = x, \text{accept}] \leq \Pr[\chi = x]$ . This inequality is less of a problem than the similar inequality  $\Pr[\zeta = z, \text{accept}] \leq \Pr[\zeta = z]$  we encountered during  $X$ -error verification, for two reasons. First, many  $X$  errors have already been eliminated, so the probabilities start out much lower. Second, overestimating the probability of an  $X$  error now is less serious; since there are no remaining postselection steps, the distribution of errors will not need to be renormalized again. Even so, we count  $X$  and  $Z$  errors together for very low-order faults, since it is relatively easy to do so.

#### 4.3.4 Error correction

An error-correction component consists of  $Z$ -error correction and  $X$ -error correction, as shown in Figure 7(b). Each sub-component begins with a pause on the input verified ancilla state, to allow for the previous postselection to complete. After extracting the error syndrome, the lowest-weight correction is computed, and this correction is applied by a change in the qubits' Pauli frames [Kni04b].

There are two types of error correction components, leading error correction (LEC) and trailing error correction (TEC). For the LEC, we may assume that the input errors  $\chi_{\text{in}}$  and  $\zeta_{\text{in}}$  are both zero. This because the probability that the rectangle is incorrect depends only on the syndrome of the output of the LEC and that syndrome depends only on the errors inside of the LEC [CDT09]. That is, we do not care about the logical state at the output of the LEC, we care only that it is correctly manipulated by the rectangle. For trailing error correction, we care only about the result of applying a logical decoder to the output. In other words, we only need to know whether the output errors  $\chi_{\text{out}}$  and  $\zeta_{\text{out}}$  represent correctable errors or not. The four relevant quantities are

$$\begin{aligned} \Pr[\chi_{\text{out}} = x_{\text{out}}, K_X = k, \text{good} | \chi_{\text{in}} = 0] & \quad \Pr[D(\chi_{\text{out}}) = d, K_X = k, \text{good} | \chi_{\text{in}} = x_{\text{in}}] \\ \Pr[\zeta_{\text{out}} = z_{\text{out}}, K_Z = k, \text{good} | \zeta_{\text{in}} = 0] & \quad \Pr[D(\zeta_{\text{out}}) = d, K_Z = k, \text{good} | \zeta_{\text{in}} = z_{\text{in}}] \end{aligned}$$

where  $d \in \{0, 1\}$  and  $D(e)$  identifies whether  $e$  is a correctable error (0) or an uncorrectable error (1). That is,  $D(e) = 1$  if and only if  $e$  decodes to a nontrivial Pauli error.

#### 4.3.5 exRec

The CNOT exRec, shown in Figure 7(a), is divided into five components: two leading error corrections, a transversal CNOT, and two trailing error corrections. At this level, we are interested in *malignant* events—the events for which the rectangle is incorrect. More specifically, when a malignant event occurs we would like to know *how* the rectangle is incorrect.

Let  $|\psi_1\rangle$  be the two-qubit state obtained by applying ideal decoders on the two blocks of the CNOT immediately following the LECs. Similarly let  $|\psi_2\rangle$  be the state obtained by applying ideal decoders immediately following the TECs. Then define  $\text{mal}_{IX}$  as the event that  $(I \otimes X)U_{\text{cnot}}|\psi_1\rangle = |\psi_2\rangle$ , where  $U_{\text{cnot}}$  is the two-qubit unitary corresponding to the ideal CNOT gate. Similarly define the events  $\text{mal}_{XI}$ ,  $\text{mal}_{XX}$ ,  $\text{mal}_{IZ}$ ,  $\text{mal}_{ZI}$ ,  $\text{mal}_{ZZ}$ . The event  $\text{mal}_E$  can be informally interpreted as the event in which the rectangle introduces a “logical” error  $E$ .

The relevant quantities are  $\Pr[M_X, K_X = k, \text{good}]$  and  $\Pr[M_Z, K_Z = k, \text{good}]$  for  $M_X \in \{\text{mal}_{IX}, \text{mal}_{XI}, \text{mal}_{XX}\}$  and  $M_Z \in \{\text{mal}_{IZ}, \text{mal}_{ZI}, \text{mal}_{ZZ}\}$ . Since we count  $X$  and  $Z$  errors separately, it is not possible to compute logical  $Y$  error quantities. Intuitively this is not a great loss, because the correlations between  $X$  and  $Z$  are much smaller at this level. In the next section we show how to use these quantities to compute a lower bound on the threshold for depolarizing noise.

### 4.4 Calculating the error threshold

As discussed in Section 1.2, the standard way of calculating the asymptotic error threshold involves finding subsets of faulty exRec locations (called “malignant”) for which some combination of Pauli errors at those locations causes the enclosed rectangle to be incorrect. Our counting method is different. We count subsets of faulty locations, but the counted information is synthesized into error probability upper bounds based on a particular noise model and error correction scheme.

In this section we outline an alternative method for rigorously lower bounding the noise threshold that is tailored specifically to the information obtained by our counting procedure. The basic idea is to treat each level-one rectangle in the level-two simulation as a single “location” with a transformed noise model based on the malignant event upper bounds obtained in [Section 4.3](#). In particular, we show how to treat each level-one exRec independently while maintaining valid upper bounds on the error probabilities.

#### 4.4.1 Calculating the pseudo-threshold

One quantity that is particularly easy to calculate from our counts is the so-called pseudo-threshold [\[SCCA06\]](#) for the CNOT location. The pseudo-threshold for location  $l$  is defined as the solution to the equation  $p = p_l^{(1)}$ , where  $p_l^{(1)}$  is the probability that the 1-Rec for location  $l$  is incorrect. We may compute a lower bound on the pseudo-threshold for CNOT by upper bounding

$$p_{\text{cnot}}^{(1)} \leq \Pr[\text{bad}|\text{accept}] + \sum_k \left( \Pr[\text{mal}_X, K_X = k, \text{good}] + \Pr[\text{mal}_Z, K_Z = k, \text{good}] \right), \quad (4.5)$$

where  $\text{mal}_X \equiv (\text{mal}_{IX} \vee \text{mal}_{XI} \vee \text{mal}_{XX})$ ,  $\text{mal}_Z \equiv (\text{mal}_{IZ} \vee \text{mal}_{ZI} \vee \text{mal}_{ZZ})$  and  $\text{accept}$  is the event that all  $X$ -error and  $Z$ -error verifications in the CNOT exRec succeed.

The pseudo-threshold is of practical interest for cases in which a finite failure probability is acceptable and only a few levels of concatenation are desired. For example, when the physical failure rate is sufficiently below the pseudo-threshold, the Golay code could be used to bootstrap into other codes with lower overhead.

The pseudo-threshold is useful to us for two reasons. First, pseudo-threshold estimates have been calculated for a variety of fault-tolerant quantum circuits including circuits based on the Golay code [\[CDT09\]](#), and therefore serve as a reference for our counting results. Second, it was conjectured by [\[SCCA06\]](#) that the pseudo-threshold is an upper bound on the asymptotic threshold. It thus provides a reasonable target for our calculation of the asymptotic threshold lower bound, which requires a noise strength maximum to be specified (see, in particular, [Appendix D.2](#)).

#### 4.4.2 Asymptotic threshold analysis

The asymptotic noise threshold is defined as the largest value  $\gamma_{\text{th}}$  such that, for all  $\gamma < \gamma_{\text{th}}$ , the probability that the fault-tolerant simulation succeeds can be made arbitrarily close to one by using sufficiently many levels of code concatenation. To prove a lower bound on the threshold we must show, in particular, that the probability of an incorrect CNOT  $k$ -Rec decreases monotonically with  $k$  for all  $\gamma < \gamma_{\text{th}}$ . Our counting technique gives an upper bound on the probability that a CNOT 1-Rec is incorrect. We now show how to upper bound incorrectness for level-two and higher and therefore lower bound  $\gamma_{\text{th}}$ .

Consider an isolated level-one CNOT exRec. Let  $\Pr[\text{mal}_E]$  be the probability that the malignant event  $\text{mal}_E$  occurs. For this event, the enclosed 1-Rec behaves as an encoded CNOT gate followed by a two-block error that, when ideally decoded, leaves a two-qubit error  $E$  on the decoded state. Then our counting technique provides upper bounds on  $\Pr[\text{mal}_E]$  for  $E \in \{IX, XI, XX, IZ, ZI, ZZ\}$ . These upper bounds can be viewed as an error model for the CNOT 1-Rec in which the correlations between  $X$  and  $Z$  errors are unknown.

We would now like to analyze the level-two CNOT exRec. Ideally, we could treat each 1-Rec in the level-two simulation as a single “location” and use the error model obtained from level-

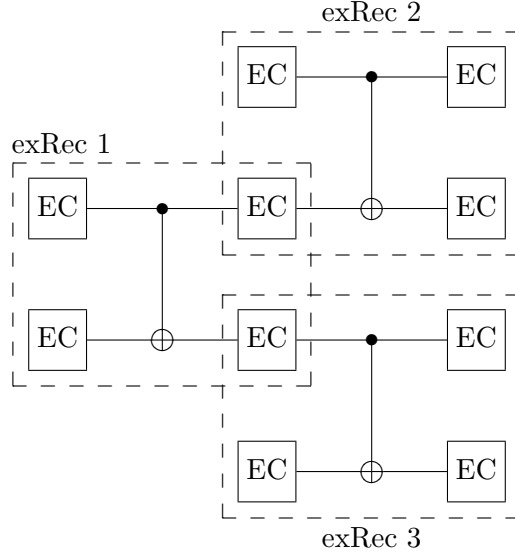


Figure 9: Overlapping exRecs: exRec 1 shares one error correction with exRec 2 and one error correction with exRec 3.

one to describe the probability of failure. Then level-two analysis could proceed by feeding this “transformed” error model back into the counting procedure in order to compute  $\Pr[\text{mal}_E]$  for the CNOT 2-Rec.

However, the transformed error model is based on analysis of an isolated level-one CNOT exRec. A typical level-one simulation will contain many exRecs, and adjacent exRecs may share error corrections at which point they can no longer be considered independently. For example, the CNOT exRec in Figure 9 shares an error correction with both of the CNOT exRecs that follow it. In [AGP06] (see also [Ali07]) this problem is solved by the following procedure known as *level reduction*:

1. Examine exRec 2. If the enclosed rectangle is incorrect then replace the entire *exRec* with a faulty version of the associated (level-zero) gate. Otherwise, replace the *rectangle* with an ideal version of the associated gate.
2. Examine exRec 3. Follow the same procedure as for exRec 2.
3. Examine exRec 1. Depending on the outcomes of exRec 2 and exRec 3, one or both of the TECs may have been removed. The enclosed rectangle now consists of the encoded CNOT and any remaining TECs. If the remains of rectangle 1 are incorrect, exRec 1 is replaced with a faulty level-zero gate. Otherwise, the rectangle is replaced with an ideal level-zero gate.

Level reduction allows the level-two analysis to proceed by treating each 1-Rec as a single *independent* location. The probability that a “location” fails in the level-two simulation is upper bounded by the probability that the corresponding 1-Rec is incorrect. The reason that level reduction works when counting sets of malignant locations is because exRecs with incorrect rectangles are replaced with faulty gates in the same way regardless of malignant event that actually occurs. The

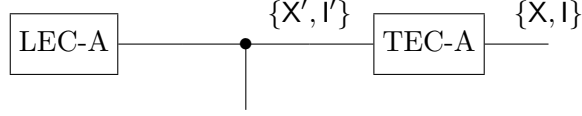


Figure 10: Upper block of the CNOT exRec. The error at the output of the TEC is either correctable ( $I$ ), or not ( $X$ ). Similarly the error immediately preceding the TEC is either correctable ( $I'$ ) or not ( $X'$ ).

quantity used to bound incorrectness probability is strictly non-increasing as locations (i.e., TECs) are removed. To see this, consider sets of exRec locations of size  $k$  and denote the set of all such sets by  $S$ . Let  $M \subseteq S$  be those sets for which some combination of nontrivial errors at the  $k$  locations causes the rectangle to be incorrect (i.e., the malignant sets). The probability that the rectangle is incorrect due to failures at exactly  $k$  locations is then no more than  $|M|p^k$ . If an error correction is removed from the exRec, some of the sets in  $M$  now contain fewer than  $k$  exRec locations. The remaining sets with  $k$  exRec locations are those that do not contain a location in the removed error correction. The number of such sets is at most  $|M|$  and so the original bound on the incorrectness probability still holds.

The disadvantage to this approach for non-adversarial noise models is that it fails to consider all of the available information. In particular, for a fixed set of malignant locations it assumes the worst-case error for each location. The probability that a given set of  $k$  locations is actually malignant can be significantly less than  $p^k$ . To obtain a more accurate analysis of the second level, we would like to replace each incorrect 1-Rec according to the malignant event that has actually occurred.

Our transformed noise model of an isolated CNOT exRec provides upper bounds on the probability of each type of malignant event, but we must show that the bounds still hold when exRecs overlap. Unfortunately, the bounds almost certainly will *not* hold. Consider, for example, the control block of the CNOT exRec, shown in Figure 10. Assume that the error immediately preceding the transversal CNOT is correctable (the error itself is not important). Let  $X$  be the event that an uncorrectable  $X$  error exists on the output of the TEC and  $I$  be the event that the error on the output is correctable. In other words  $X \equiv (\text{mal}_{XI} \vee \text{mal}_{XX})$  and  $I \equiv \neg X$ . Then define  $X' \equiv \neg I'$  as the event that a correctable  $X$  error exists on the block following the transversal CNOT but before error correction.  $\Pr[\text{mal}_{XI}]$  will be non-increasing when removing the trailing error correction only if  $\Pr[X'] \leq \Pr[X]$ . On the other hand,  $\Pr[\text{mal}_{IX}]$  will be non-increasing only if  $\Pr[I'] \leq \Pr[I]$ . Since  $\Pr[X] + \Pr[I] = \Pr[X'] + \Pr[I'] = 1$ , both conditions are satisfied only if  $\Pr[X] = \Pr[X']$  and  $\Pr[I] = \Pr[I']$ , which of course is highly unlikely.

In order to ensure a proper upper bound on each of the malignant event probabilities, we must calculate upper bounds for the complete exRec and for incomplete exRecs in which one or more trailing error corrections have been removed. Calculations for the complete exRec were discussed in Section 4.3. Calculations for the incomplete exRecs are the same except that some of the TEC components are not considered. Bounding the malignant event probability is a matter of finding a polynomial that bounds all four cases (see Appendix D.2).

Once proper bounds on the level-one malignant event probabilities are determined, we would like to plug the transformed error model into our counting procedure in order to determine the level-two error probabilities. There are a few things to consider before doing so. First, part of the counting strategy relies on using the correlations between  $X$  and  $Z$  errors in order to make corrections for over-counting that occurs during postselection. The transformed error model, however, contains no

such correlation information, so these corrections must be omitted. Second, the CNOT malignant event upper bounds do not contain information about rest, preparation or measurement locations. Level-one error models for these locations can be computed using the same counting strategy as the CNOT, but with an appropriately modified exRec.<sup>1</sup>

Finally, in the depolarizing noise model, the error probabilities of each location are constant multiples of the noise strength  $\gamma$ . Our upper bounds on the malignant event probabilities, however, need not have any scalar relationship. For computer analysis, error probabilities must be re-normalized in terms of  $\gamma$  and error weights recalculated as follows. Let  $\mathcal{P}_E^{(1)}$  be our upper bound on the level-one malignant event  $\text{mal}_E$ . Then construct a polynomial  $\Gamma^{(1)}$  and choose constants  $\alpha_E$  such that

$$\mathcal{P}_E^{(1)}(\gamma) \leq \alpha_E \Gamma^{(1)}(\gamma) \quad (4.6)$$

for all  $E$ . The polynomial  $\Gamma^{(1)}$  can be viewed as an effective noise strength “reference” for level-one.  $\Gamma^{(1)}(\gamma)$  is a function of  $\gamma$ , but we will usually denote it as  $\Gamma^{(1)}$  for convenience of notation. Together with weights  $\alpha_E$ ,  $\Gamma^{(1)}$  defines a noise model similar to the depolarizing noise model defined in Section 4.1. See Appendix D for details of the construction.

Now the new error model is input into the counting procedure and upper bounds on the level-two error rates are computed. Let  $\mathcal{P}_E^{(2)}(\Gamma)$  be the upper bound computed for  $\text{mal}_E$  at level-two. Then we have the following conditions on the level-one and level-two malignant event probabilities:

$$\begin{aligned} \Pr[\text{mal}_E^{(1)}] &\leq \mathcal{P}_E^{(1)}(\gamma) \leq \alpha_E \Gamma^{(1)} \\ \Pr[\text{mal}_E^{(2)}] &\leq \mathcal{P}_E^{(2)}(\Gamma^{(1)}) . \end{aligned} \quad (4.7)$$

We also claim that  $\mathcal{P}_E^{(2)}$  obeys the following property:

**Claim 4.2.** For  $0 \leq \epsilon \leq 1$ ,  $\mathcal{P}_E^{(2)}(\epsilon \Gamma^{(1)}(\gamma)) \leq \epsilon^4 \mathcal{P}_E^{(2)}(\Gamma^{(1)}(\gamma))$ .

Proof of this claim is based on the form of the polynomials constructed by our counting technique and the fact that our circuits are strictly fault-tolerant. Details of the proof are delegated to Appendix D.3.

We are now in a position to establish conditions for a noise threshold, i.e., the conditions under which the probability of a successful simulation can be made arbitrarily close to one.

**Theorem 4.3.** Let  $M$  be the set of all level-one CNOT, preparation, measurement and rest malignant events consisting of:  $\text{mal}_{IX}$ ,  $\text{mal}_{XI}$ ,  $\text{mal}_{XX}$ ,  $\text{mal}_{IZ}$ ,  $\text{mal}_{ZI}$ ,  $\text{mal}_{ZZ}$ ,  $\text{mal}_X^{\text{prep}}$ ,  $\text{mal}_Z^{\text{prep}}$ ,  $\text{mal}_X^{\text{meas}}$ ,  $\text{mal}_Z^{\text{meas}}$ ,  $\text{mal}_X^{\text{rest}}$  and  $\text{mal}_Z^{\text{rest}}$ . Also let  $\mathcal{P}_E^{(1)}$ ,  $\mathcal{P}_E^{(2)}$  and  $\Gamma^{(1)}$  be polynomials and  $\alpha_E$  constants as discussed above. Then the tolerable noise threshold for depolarizing noise is lower bounded by the largest value  $\gamma_{th}$  such that

$$\mathcal{P}_E^{(2)}(\Gamma^{(1)}(\gamma_{th})) \leq \alpha_E \Gamma^{(1)}(\gamma_{th}) \quad (4.8)$$

for all  $\text{mal}_E \in M$ .

*Proof.* Assume that  $\mathcal{P}_E^{(2)}(\Gamma^{(1)}) < \alpha_E \Gamma^{(1)}$ , for all  $\text{mal}_E$  and  $\gamma \in (0, \gamma_{th})$ . Then, for a fixed  $\gamma \in [0, \gamma_{th})$ , there exists some positive  $\epsilon < 1$  such that, for all malignant events  $\text{mal}_E$ ,  $\mathcal{P}_E^{(2)}(\Gamma^{(1)}) \leq \epsilon \alpha_E \Gamma^{(1)}$ .

By choosing  $\Gamma^{(2)} := \epsilon \Gamma^{(1)}$  we obtain an effective noise model for level two in which the weights  $\alpha_E$  are unchanged. Since our counting method depends only on the error weights, the polynomials that

---

<sup>1</sup>Alternatively, they can be incorporated into the CNOT exRecs [AC07].



Verification schedule	CNOT Pseudothreshold	Threshold
Steane-4	$1.72 \times 10^{-3}$	$1.24 \times 10^{-3}$
Overlap-4	$1.73 \times 10^{-3}$	$1.32 \times 10^{-3}$

Table 7: Threshold lower bounds for circuits based on our four-ancilla preparation and verification schedules for the Golay code. Thresholds are given with respect to  $p$  the probability that a physical CNOT gate fails, according to the depolarizing noise model defined in [Section 4.1](#)

upper bound the level-three malignant events will be the same as the polynomials that upper bound the level-two malignant events. That is,  $\mathcal{P}_E^{(3)}(\Gamma) = \mathcal{P}_E^{(2)}(\Gamma)$ . Thus,

$$\Pr[\text{mal}_E^{(3)}] \leq \mathcal{P}_E^{(3)}(\Gamma^{(2)}) = \mathcal{P}_E^{(2)}(\epsilon\Gamma^{(1)}) < \epsilon^5 \alpha_E \Gamma^{(1)} , \quad (4.9)$$

where the last inequality follows from [Claim 4.2](#). Repeating this process  $k$  times yields

$$\Pr[\text{mal}_E^{(k+1)}] \leq \mathcal{P}_E^{(k+1)}(\Gamma^{(k)}) < \epsilon^{4k-3} \alpha_E \Gamma^{(1)} , \quad (4.10)$$

which approaches zero in the limit of large  $k$ .  $\square$

Testing of the assumption  $\mathcal{P}_E^{(2)}(\Gamma^{(1)}) < \alpha_E \Gamma^{(1)}$  over a fixed interval  $(0, \gamma_{\text{th}})$  is straightforward because, as discussed in [Appendix C](#), all of our malignant event polynomials (including  $\Gamma^{(1)}$ ) are monotone non-decreasing up to sufficiently large values of  $\gamma$ .

## 4.5 Results: Threshold lower bounds

Threshold results were obtained by implementing our counting technique as a collection of modules written in Python and C; the source code is available at [\[PR11\]](#). Rigorous threshold lower bounds for both of our four-ancilla preparation and verification circuits are given in [Table 7](#). The main program takes as input the four-ancilla preparation circuits, the noise model, and the good and bad event settings. It outputs, for each type of exRec and each malignant event, a polynomial representing an upper bound on the event probability. See [Figure 11](#). These polynomials are either evaluated directly to calculate the pseudo-threshold, or processed into a transformed error model and fed back into the program.

The Python modules are broken up according to the components described in [Section 4.3](#). The main task for each component is, for each error equivalence class, to compute a weighted count of location sets that produce that error. Counts for each component are obtained by first computing counts for all of its sub-components and then convolving the results. Details are discussed in [Appendix B](#).

The most time consuming part of the computation involved the CNOT exRec component. Computing weighted counts for this component required a custom convolution with nearly four trillion combinations. This part of the program was written in C to save time. Even so, running the entire program to completion for a fixed ancilla preparation and verification schedule on 31 cores in parallel took about four days.

Our thresholds compare favorably to threshold results for similar circuits. For a six-ancilla preparation and verification circuit, Aliferis and Cross [\[AC07\]](#) give a threshold estimate based on malignant set sampling of  $p \approx 1 \times 10^{-4}$  for adversarial noise. Our results beat this by an order

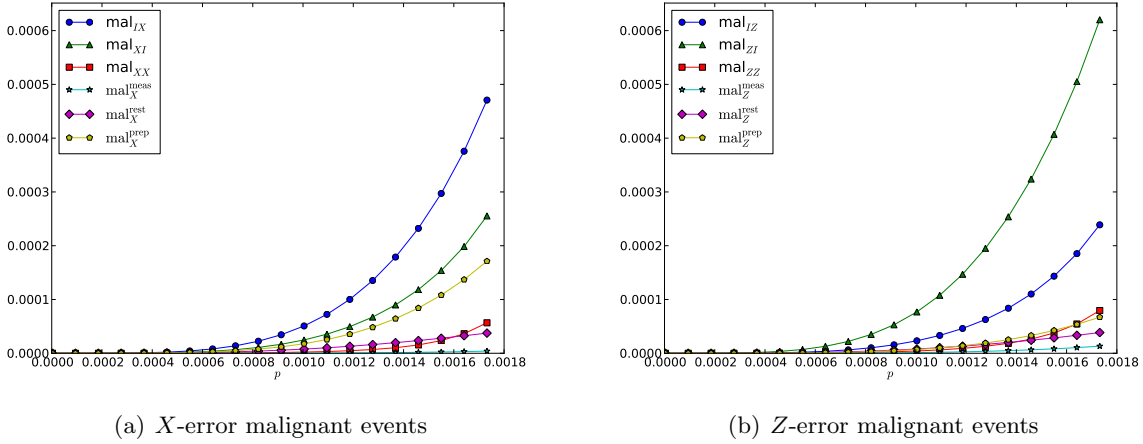


Figure 11: These plots show upper bounds on probability of malignant events for the different level-one exRecs. The  $\text{mal}_{IX}$ ,  $\text{mal}_{XI}$ ,  $\text{mal}_{XX}$ ,  $\text{mal}_{IZ}$ ,  $\text{mal}_{ZI}$  and  $\text{mal}_{ZZ}$  events all pertain to the CNOT exRec; the  $\text{mal}_X^{\text{prep}}$  and  $\text{mal}_Z^{\text{prep}}$  events correspond to the  $|0\rangle$  and  $|+\rangle$  preparation exRecs, respectively;  $\text{mal}_X^{\text{meas}}$  and  $\text{mal}_Z^{\text{meas}}$  correspond to  $Z$ -basis and  $X$ -basis measurement exRecs;  $\text{mal}_X^{\text{rest}}$  and  $\text{mal}_Z^{\text{rest}}$  pertain to the rest exRecs. Note that the upper bound on  $\text{mal}_{ZI}$  is significantly higher than that of its dual counterpart  $\text{mal}_{IX}$ . This is due largely to the arbitrary choice in error correction to correct  $Z$  errors first and  $X$  errors second.

of magnitude and provide strong evidence that that our counting technique is an improvement over malignant set sampling and malignant set counting for the case of depolarizing noise. Our results also essentially close the gap with other analytical and Monte Carlo threshold estimates for depolarizing noise. Using a closed form analysis, Steane [Ste03] estimated a threshold on the order of  $10^{-3}$  for the Golay code with similar noise parameters. Cross et al. [CDT09] estimated a pseudo-threshold of  $2.25 \times 10^{-3}$  based on Monte Carlo simulations of a twelve-ancilla preparation and verification circuit.

Beyond circuits based on the Golay code, our results may be the highest rigorous threshold lower bounds known. Aliferis et al. [AGP08] prove a lower bound of  $p \geq 1.04 \times 10^{-3}$  for a slightly stronger noise model based a certain kind of stochastic noise. Their analysis applies to teleportation-based gates due to Knill [Kni04b] in which Bell pairs encoded into an error correcting code  $C_2$  are prepared by first encoding each qubit of the  $C_2$  block into an error *detecting* code  $C_1$  and performing error detection and postselection after each step of the  $C_2$  encoding. Our thresholds are only about 20 to 25 percent better, but apply to circuits that require far less overhead. This implies only that, in the depolarizing noise model our analysis is more accurate, and not that our schemes tolerate more noise.

The limiting factor on the threshold value is the event  $\text{mal}_{ZI}$ . That is,  $\text{mal}_{ZI}$  is the event  $E$  for which  $\Pr[\text{mal}_E^{(2)}] = \Pr[\text{mal}_E^{(1)}]$  takes the smallest value of  $p$ . In fact, the corresponding threshold values for nearly all  $Z$ -error malignant events are lower than threshold values for *any* of the  $X$ -error events. This asymmetry is due to the arbitrary order with which we perform error correction— $Z$  first, then  $X$ . Some  $X$  errors resulting from the leading  $Z$ -error correction will be corrected by the  $X$ -error correction that follows. However,  $Z$  errors resulting from the  $X$ -error correction may propagate through the encoded operation before arriving at the  $Z$ -error correction on the trailing end. As a result, it is more likely for  $Z$  errors on individual blocks to be combined by the CNOT

gate and create an uncorrectable error. Evidence of this effect can be seen in the level-one malignant event probabilities shown in [Figure 11](#).

It should be possible to reduce such lopsided event probabilities by customizing the error correction order for each EC based on the specifics of the ancilla preparation circuits. However, analyzing such a scheme would require consideration of up to 36 different full or partial CNOT exRecs (two choices for each EC) instead of four and is likely to yield only a small improvement in the threshold. Note that other small improvements could be made by, for example, eliminating measurement or rest exRecs at level-two. For simplicity, these optimizations were not considered.

## 5 Future work

We have shown two alternative circuits for the fault-tolerant preparation of Golay encoded ancillas. Our circuits require a total of only four encoded ancillas, and thus outperform the previous best known circuits in terms of overhead. We have also demonstrated a new malignant set counting technique and threshold analysis tailored specifically for depolarizing noise. With this technique, we proved a tolerable noise threshold of  $1.32 \times 10^{-3}$ , the highest rigorous threshold known.

There are a number areas for future work. First, using the overlap encoding method given in [Section 3.2](#), we were able to reduce the number of CNOT gates when compared to the standard encoding procedure. However, the circuit given in [Figure 4](#) was constructed by hand and is not necessarily optimal. It would be ideal have an algorithm for finding a preparation circuit with the fewest number of CNOT gates. Second, our techniques for optimizing verification circuit overhead could be applied to other large codes. For example, the self-dual BCH  $[[47, 1, 11]]$  and concatenated Steane  $[[49, 1, 9]]$  codes (see, e.g., [\[GB99\]](#)) are similar in nature to the Golay code and may yield similar results. Variations of the verification procedure could also be analyzed. Overhead might be reduced by, for example, attempting to correct some errors detected during verification rather than always scrapping the entire procedure.

Another possible avenue of interest is to apply our malignant set counting technique to other types of fault-tolerant error correction methods. In particular, the teleportation-based schemes due to Knill are enticing candidates. Simulations indicate that these schemes can tolerate a depolarizing noise rate as high as  $p = 1\%$ ; the best rigorous lower bound is  $p \geq 1.04 \times 10^{-3}$  [\[AGP08\]](#), but assumes a stronger noise model. By analyzing depolarizing noise directly, our technique might provide a tighter bound. However, teleportation-based schemes introduce new analytical challenges. In particular, the teleportation-based CNOT gadget is implemented using two Bell pairs and would require simultaneous tracking six blocks instead of just two. Additionally, certain schemes may require counting of Hadamard and non-transversal single qubit gadgets, further complicating the analysis.

## References

- [AB97] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error rate. In *Proc. 29th ACM Symp. on Theory of Computing (STOC)*, pages 176–188, 1997, [arXiv:quant-ph/9906129](#).
- [AC07] Panos Aliferis and Andrew W. Cross. Subsystem fault tolerance with the Bacon-Shor code. *Phys. Rev. Lett.*, 98:220502, 2007, [arXiv:quant-ph/0610063](#).

- [AGP06] Panos Aliferis, Daniel Gottesman, and John Preskill. Quantum accuracy threshold for concatenated distance-3 codes. *Quant. Inf. Comput.*, 6:97–165, 2006, [arXiv:quant-ph/0504218](#).
- [AGP08] Panos Aliferis, Daniel Gottesman, and John Preskill. Accuracy threshold for postselected quantum computation. *Quant. Inf. Comput.*, 8:181–244, 2008, [arXiv:quant-ph/0703264](#).
- [Ali07] Panos Aliferis. *Level reduction and the quantum threshold theorem*. PhD thesis, California Institute of Technology, 2007, [arXiv:quant-ph/0703230](#).
- [BK05] Sergey Bravyi and Alexei Yu. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71:022316, 2005, [arXiv:quant-ph/0403025](#).
- [CDT09] Andrew W. Cross, David P. DiVincenzo, and Barbara M. Terhal. A comparative code study for quantum fault-tolerance. 2009, [arXiv:0711.1556](#).
- [DA07] David P. DiVincenzo and Panos Aliferis. Effective fault-tolerant quantum computation with slow measurements. *Phys. Rev. Lett.*, 98(2):020501, 2007, [arXiv:quant-ph/0607047](#).
- [DKLP02] Eric Dennis, Alexei Yu. Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43(9):4452–4505, 2002, [arXiv:quant-ph/0110143](#).
- [GB99] Markus Grassl and Thomas Beth. Quantum BCH Codes. In *Proc. 10th Int. Symp. on Theoretical Electrical Engineering (ISTET)*, pages 207–212, 1999, [arXiv:quant-ph/9910060](#).
- [Haz90] M Hazewinkel. *Encyclopaedia of mathematics: an updated and annotated translation of the Soviet Mathematical encyclopaedia*, volume 6. Springer, 1990.
- [IWPk08] Nemanja Isailovic, Mark Whitney, Yatish Patel, and John Kubitowicz. Running a Quantum Circuit at the Speed of Data. In *Proc. 35th Int. Symp. on Computer Architecture (ISCA)*, pages 177–188, 2008, [arXiv:0804.4725](#).
- [Kit97] Alexei Yu. Kitaev. Quantum computations: algorithms and error correction. *Russian Math. Surveys*, 52(6):1191–1249, 1997.
- [KL96] Emanuel Knill and Raymond Laflamme. Concatenated quantum codes. 1996, [arXiv:quant-ph/9608012](#).
- [Kni04a] Emanuel Knill. Fault-tolerant postselected quantum computation: schemes, 2004, [arXiv:quant-ph/0402171](#).
- [Kni04b] Emanuel Knill. Quantum computing with realistically noisy devices. *Nature*, 434:39–44, 2004, [arXiv:quant-ph/0410199](#).
- [PR11] Adam Paetznick and Ben W. Reichardt. qfault: Python modules for counting malignant sets of locations in fault-tolerant quantum circuits. <http://code.google.com/p/qfault/>, 2011.

- [Rei04] Ben W. Reichardt. Improved ancilla preparation scheme increases fault-tolerant threshold, 2004, [arXiv:quant-ph/0406025](#).
- [RH07] Robert Raussendorf and Jim Harrington. Fault-tolerant quantum computation with high threshold in two dimensions. *Phys. Rev. Lett.*, 98:190504, 2007, [arXiv:quant-ph/0610082](#).
- [RHG06] Robert Raussendorf, Jim Harrington, and Kovid Goyal. A fault-tolerant one-way quantum computer. *Ann. Phys.*, 321(2242), 2006, [arXiv:quant-ph/0510135](#).
- [SCCA06] K. M. Svore, A. W. Cross, I. L. Chuang, and A. V. Aho. A flow-map model for analyzing pseudothresholds in fault-tolerant quantum computing. *Quant. Inf. Comput.*, 6(3):193–212, 2006, [arXiv:quant-ph/0508176](#).
- [Sho96] Peter W. Shor. Fault-tolerant quantum computation. In *Proc. 37th Symp. on Foundations of Computer Science (FOCS)*, pages 56–65, 1996, [arXiv:quant-ph/9605011](#).
- [Ste97] Andrew M. Steane. Active stabilization, quantum computation, and quantum state synthesis. *Phys. Rev. Lett.*, 78(11):2252–2255, 1997, [arXiv:quant-ph/9611027](#).
- [Ste02] Andrew M. Steane. Fast fault-tolerant filtering of quantum codewords, 2002, [arXiv:quant-ph/0202036](#).
- [Ste03] Andrew M. Steane. Overhead and noise threshold of fault-tolerant quantum error correction. *Phys. Rev. A*, 68:042322, 2003, [arXiv:quant-ph/0207119](#).
- [Ste07] Andrew M. Steane. How to build a 300 bit, 1 Giga-operation quantum computer. *Quantum Inf. Comput.*, 7(3):171–183, 2007, [arXiv:quant-ph/0412165](#).
- [Zal97] Christof Zalka. Threshold estimate for fault tolerant quantum computation, 1997, [arXiv:quant-ph/9612028](#).

## A Component counting

### A.1 Bounding bad events

Bad fault events are defined, in part, by establishing some limit  $k_{\text{good}}$  on the number of failures  $K$  within the component. In the  $X$ -error case,  $|+\rangle$  preparation and  $X$ -basis measurement locations are ignored (they cannot produce  $X$  errors). For a component containing  $n_c$  CNOT gates,  $n_r$  rests, and  $n_p + n_m = n_{pm}$   $|0\rangle$  preparations and  $Z$ -basis measurements, let  $A_{\vec{n}}$  and  $\beta_{\vec{n}}(\vec{k})$  and be defined as

$$\begin{aligned}
 A_{\vec{n}} &= (1 - 12\gamma)^{n_c} (1 - 8\gamma)^{n_r} (1 - 4\gamma)^{n_{pm}} \\
 \beta_{\vec{n}}(\vec{k}) &= \binom{n_c}{k_c} \binom{n_r}{k_r} \binom{n_{pm}}{k_{pm}} .
 \end{aligned} \tag{A.1}$$

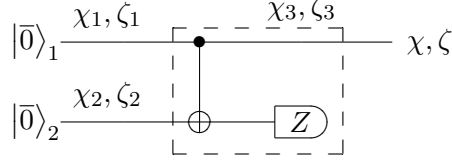


Figure 12:  $X$ -error verification. The  $X$ -error verification component consists of two Golay encoded  $|\bar{0}\rangle$  preparations, a transversal CNOT and a transversal  $Z$ -basis measurement.  $X$  ( $\chi_i$ ) and  $Z$  ( $\zeta_i$ ) errors for each part are labeled. The output is an  $X$  error  $\chi$  and  $Z$  error  $\zeta$ .

Then the probability of more than  $k_{\text{good}}$   $X$  failures is

$$\begin{aligned} \Pr[k_{\text{good}} < K_X < k_{\text{max}}] &= A_{\vec{n}} \sum_{k_{\text{good}} < |\vec{k}| < k_{\text{max}}} \beta_{\vec{n}}(\vec{k}) \left( \frac{12\gamma}{1-12\gamma} \right)^{k_c} \left( \frac{8\gamma}{1-8\gamma} \right)^{k_r} \left( \frac{4\gamma}{1-4\gamma} \right)^{k_{pm}} \\ &\leq A_{\vec{n}} \sum_{k_{\text{good}} < |\vec{k}| < k_{\text{max}}} \beta_{\vec{n}}(\vec{k}) \left( \frac{\gamma}{1-12\gamma} \right)^{|\vec{k}|} 12^{k_c} 8^{k_r} 4^{k_{pm}}. \end{aligned} \quad (\text{A.2})$$

The sums are over all possible failure partitions  $\vec{k} = (k_c, k_r, k_{pm})$  for which  $|\vec{k}| = k_c + k_r + k_{pm}$  is in the correct range. The failure partition represents the number of CNOT failures  $k_c$ , rest failures  $k_r$ , and preparation and measurement failures  $k_{pm} = k_p + k_m$ . The upper bound  $k_{\text{max}}$  is used to avoid double counting between components and sub-components, and may be omitted in which case take  $k_{\text{max}} = n_c + n_r + n_{pm} + 1$ . For components with a large number of locations, it is convenient to approximate (A.2) by evaluating the sum up to only a fixed number of failures  $k' = k_{\text{good}} + \text{const.}$  and then upper bounding the rest of the sum by

$$\Pr[k' < K_X] \leq \sum_{\vec{k}: |\vec{k}| = k' + 1} \beta_{\vec{n}}(\vec{k}) (12\gamma)^{k_c} (8\gamma)^{k_r} (4\gamma)^{k_{pm}}. \quad (\text{A.3})$$

This bound is easy to compute, so long as the number of sub-components is reasonable, and is better than the simpler bound  $\binom{n}{k'+1} (12\gamma)^{k'+1}$ .

The  $Z$ -error case is completely analogous except that now  $|+\rangle$  and  $X$ -basis measurement locations are counted and  $|0\rangle$  preparation and  $Z$ -basis measurement locations are ignored. All of the equations remain the same.

## A.2 $X$ -error verification

The  $X$ -error verification component is illustrated in Figure 12. It includes three sub-components that fail independently. Let  $(\chi_1, \zeta_1)$  be the  $X$  and  $Z$  errors resulting from the first  $|\bar{0}\rangle$  preparation and  $(\chi_2, \zeta_2)$  be the errors from the second  $|\bar{0}\rangle$  preparation. Let  $(\chi_3, \zeta_3)$  be the errors on the remaining transversal CNOT and  $Z$ -basis measurement locations; we will denote by  $(\chi'_3, \zeta'_3)$  the portion of these errors on the control (upper) code block, and  $(\chi''_3, \zeta''_3)$  the errors on the target (lower) code block. Denote the final output errors by  $(\chi, \zeta)$ .

Define sub-component  $j$  to be  $\text{bad}_Z^{(j)}$  if it contains five or more  $Z$  failures. If the sub-component is not  $\text{bad}_Z^{(j)}$ , it is  $\text{good}_Z^{(j)}$ . Similarly define  $\text{bad}_X^{(j)}$  and  $\text{good}_X^{(j)}$  for  $X$  failures.

Define the  $X$ -error verification component to be “ $\text{bad}_Z$ ” if any of the sub-components are  $\text{bad}_Z^{(j)}$ , or there are more than six  $Z$  failures. If the component is not  $\text{bad}_Z$ , it is  $\text{good}_Z$ . Similarly define  $\text{bad}_X$  and  $\text{good}_X$  for  $X$  failures. Define the  $X$ -error verification component to be “ $\text{best}$ ” if there are fewer than four failures of any kind.

The quantities that we will compute for an  $X$ -error verification component are:

$$\Pr[(\chi, \zeta) = (x, z), K = k, \text{best} | \text{accept}], \Pr[\chi = x, K_X = k, \text{good}_X | \text{accept}], \\ \Pr[\zeta = z, K_Z \leq k, \text{good}_Z | \text{accept}], \Pr[\text{bad}_X | \text{accept}] \text{ and } \Pr[\text{bad}_Z | \text{accept}] .$$

Here, for example, the first quantity is the probability of  $X$ -error  $x$  and  $Z$ -error  $z$  occurring with exactly  $k$  failures and the  $\text{best}$  event, conditioned on  $X$ -error verification accepting (the event  $\text{accept}$ ). The second and third quantities are similar, except tracking only  $X$  or  $Z$  errors, respectively.

Begin by placing a lower bound on the probability of the event  $\text{accept}$  that no  $X$  errors are detected. Define  $\text{out}(x) := \{\vec{x} : x_1 x'_3 \equiv x\}$ ,  $\text{out}(z) := \{\vec{z} : z_1 z_2 z'_3 \equiv z\}$  and  $\text{accept}_X := \{\vec{x} : x_1 x_2 x''_3 \equiv 0\}$ . Use

$$\Pr[\text{accept}] \geq \Pr[\text{accept}, \text{good}_X] = 1 - \Pr[\neg \text{accept}, \text{good}_X] - \Pr[\text{bad}_X] \quad (\text{A.4})$$

and

$$\Pr[\neg \text{accept}, \text{good}_X] \leq \sum_{\substack{k \leq 6, |\vec{k}|=k \\ \vec{x} \notin \text{accept}_X}} \prod_{j=1}^3 \Pr[\chi_j = x_j, K_{X,j} = k_j, \text{good}_X^{(j)}] . \quad (\text{A.5})$$

Here, the sum is over all possible divisions  $\vec{k} = (k_1, k_2, k_3)$  of the number of failures among the three sub-components, and of  $X$  errors that lead to a nontrivial syndrome measurement; it is a discrete convolution of the error probabilities. Figure 16(a) shows computed lower bounds on  $\Pr[\text{accept}]$  for one particular ancilla preparation and verification circuit.

The calculations we relate here and in the sequel are generally dictated by constraints of combinatorial complexity. In Eq. (A.5), for instance, the number of terms in the sum is, naïvely, on the order of  $(2^{12})^4 \cdot 3^6 \approx 2 \times 10^{17}$ , since there are  $2^{12}$  inequivalent  $X$  errors on a single code block. Summing so many terms would be infeasible. In fact, though, the number of inequivalent  $X$  errors produced by an ancilla preparation circuit with  $k \leq 2$  faults is much less than  $2^{12}$ . For ancillas prepared using Figure 4, there are 58 inequivalent  $X$  errors created with  $k = 1$ , and 1225 created for  $k = 2$ . The number of inequivalent  $X$  errors for the transversal CNOT scales as  $\binom{23}{k} 3^k$ . Since the number of possible partitions of  $k$  faults into  $m$  components is  $O(k^m)$ , the worst case partition with  $|\vec{k}| = 6$ ,  $\vec{k} = (1, 2, 3)$ , involves only about  $3 \times 10^9$  error combinations. The bound in (A.5) can therefore be computed with relative ease. This combinatorial analysis is very similar for the other equations below.

We similarly compute for  $k \in \{0, 1, 2, 3\}$ ,

$$\Pr[(\chi, \zeta) = (x, z), K = k, \text{best}, \text{accept}] = \sum_{\substack{|\vec{k}|=k \\ \vec{x} \in \text{out}(x) \cap \text{accept}_X \\ \vec{z} \in \text{out}(z)}} \prod_{j=1}^3 \Pr[(\chi_j, \zeta_j) = (x_j, z_j), K_j = k_j] , \quad (\text{A.6})$$

and for  $k \in \{0, \dots, 6\}$ ,

$$\Pr[\chi = x, K_X = k, \text{good}_X, \text{accept}] = \sum_{\substack{|\vec{k}|=k \\ \vec{x} \in \text{out}(x) \cap \text{accept}_X}} \prod_{j=1}^3 \Pr[\chi_j = x_j, K_{X,j} = k_j, \text{good}_X^{(j)}] . \quad (\text{A.7})$$



It is more difficult to compute  $\Pr[\zeta = z, K_Z = k, \text{good}_Z, \text{accept}]$  accurately. The naïve bound  $\Pr[\zeta = z, K_Z = k, \text{good}_Z, \text{accept}] \leq \Pr[\zeta = z, K_Z = k, \text{good}_Z]$  is quite poor, since  $X$ -error verification catches many  $Z$  faults that occur with  $X$  faults, i.e., as a  $Y$  fault. The problem, though, is that we lack  $X$ -error information with which to determine whether verification is successful or not. Therefore we use instead the bound

$$\Pr[\zeta = z, K_Z \leq k, \text{good}_Z | \text{accept}] \leq \frac{\Pr[\zeta = z, K_Z \leq k, \text{good}_Z] - \Pr[\zeta = z, K \leq k, \text{best}, \neg \text{accept}]}{\Pr[\text{accept}]}, \quad (\text{A.8})$$

which holds because **best** is a subset of **good<sub>Z</sub>**. The numerator can be decomposed as

$$\Pr[\zeta = z, K_Z \leq k, \text{good}_Z] - \Pr[\zeta = z, K \leq k, \text{best}, \neg \text{accept}] = \sum_{k'=0}^k \mathcal{P}(z, k') \quad (\text{A.9})$$

where

$$\mathcal{P}(z, k) := \Pr[\zeta = z, K_Z = k, \text{good}_Z] - \sum_x \Pr[(\chi, \zeta) = (x, z), K = k, \text{best}, \neg \text{accept}]. \quad (\text{A.10})$$

The first term of (A.10) represents the pessimistic assumption that all  $Z$  errors pass verification under the  $Z$ -only noise model. It does not require any  $X$ -error information and may be computed in the same way as Eqs. (A.6) and (A.7):

$$\Pr[\zeta = z, K_Z = k, \text{good}_Z] = \sum_{\substack{|\vec{k}|=k \\ \vec{z} \in \text{out}(z)}} \prod_{j=1}^3 \Pr[\zeta_j = z_j, K_Z = k_j, \text{good}_Z^{(j)}]. \quad (\text{A.11})$$

The second term uses the full  $XZ$  noise model and corrects the over-counting of the first term by subtracting off most of correlated  $Z$  errors that are rejected. It is nearly identical to (A.6) except that the *rejected* errors are counted instead of the accepted errors. It is computed as

$$\Pr[(\chi, \zeta) = (x, z), K = k, \text{best}, \neg \text{accept}] = \sum_{\substack{|\vec{k}|=k \\ \vec{x} \in \text{out}(x) \setminus \text{accept}_X \\ \vec{z} \in \text{out}(z)}} \prod_{j=1}^3 \Pr[(\chi_j, \zeta_j) = (x_j, z_j), K_j = k_j]. \quad (\text{A.12})$$

To get a quantitative estimate of the significance of this correction, we show in Table 8 the sum of (A.11) and (A.12) over all nontrivial  $Z$  errors for  $p = 10^{-3}$ . From this table, we compute a ratio  $\Pr[\zeta \neq 0, \text{best}, \neg \text{accept}] / \Pr[\zeta \neq 0, \text{good}_Z]$  of about 0.57, indicating that, as expected, the correction cuts the probability of a  $Z$  error roughly in half. First-order quantities account for most of the correction. Third-order quantities are negligible, providing further justification for our choice of  $k_{\text{best}} = 3$ .

We see from Figure 16(a) that the lower bound on  $Z$ -error verification acceptance at  $p = 10^{-3}$  is about 0.84. The correction eliminates better than half of the  $Z$  errors going into  $Z$ -error verification, so we crudely estimate a lower bound *without* the correction of about 0.63, a decrease by a factor of 1.3. There are four  $Z$ -error verifications of encoded  $|0\rangle$  in the (full) exRec and four similar  $X$ -error verifications of encoded  $|+\rangle$ . Thus, in the normalization factor alone, the correction reduces upper bounds on the malignant event probabilities (see (A.23)) by roughly a factor of  $1.3^8 \approx 8$ . The savings is less, of course, as  $p$  decreases.

Finally, bound the probability of the **bad<sub>X</sub>** event by  $\Pr[\text{bad}_X] \leq \Pr[K_X > 6] + \sum_j \Pr[\text{bad}_X^{(j)}]$ , and use  $\Pr[\text{bad}_X | \text{accept}] \leq \Pr[\text{bad}_X] / \Pr[\text{accept}]$ . The probability of the **bad<sub>Z</sub>** event is similarly bounded.

	$k = 1$	$k = 2$	$k = 3$	$k = 4$	$k = 5$	$k = 6$
$\Pr[\zeta \neq 0, K_Z = k, \text{good}_Z]$	0.1228	0.0101	0.0005	$2 \times 10^{-5}$	$6 \times 10^{-7}$	$1 \times 10^{-8}$
$\Pr[\zeta \neq 0, K = k, \text{best}, \neg \text{accept}]$	0.0614	0.0140	0.0012	-	-	-

Table 8: This table shows the (un-normalized) probability that a non-trivial  $Z$  error occurs during  $X$ -error verification of  $|\bar{0}\rangle_1$  for the Overlap-4 verification schedule, evaluated at  $p = 10^{-3}$ . The first row gives upper bounds on the probability of a nontrivial  $Z$ -error under the  $Z$ -only noise model, assuming that all  $Z$  errors pass verification. The second row gives lower bounds on the correction applied in (A.8) based on the full depolarizing noise model.

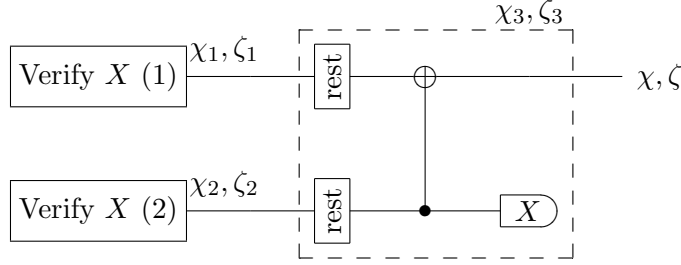


Figure 13:  $Z$ -error verification. The  $Z$ -error verification component consists of two  $X$ -error-verified ancillas, two transversal rest operations, a transversal CNOT and a transversal  $X$ -basis measurement.

### A.3 $Z$ -error verification

The  $Z$ -error verification component is illustrated in Figure 13 with its three labeled independent sub-components. Define the component to be  $\text{bad}_X$  if any of the sub-components are  $\text{bad}_X$  or there are more than seven  $X$  failures. The  $\text{bad}_X$  events for sub-components one and two are defined in Appendix A.2 and  $\text{bad}_X^{(3)}$  occurs when component three contains more than four  $X$  failures. Thus  $\Pr[\text{bad}_X] \leq \Pr[K > 7] + \sum_{j=1}^3 \Pr[\text{bad}_X^{(j)}]$ . Similarly define  $\text{bad}_Z$  for  $Z$  failures. Also define  $\text{out}(x) := \{\vec{x} : x_1 x_2 x'_3 \equiv x\}$ ,  $\text{out}(z) := \{\vec{z} : z_1 z'_3 \equiv z\}$  and  $\text{accept}_Z := \{\vec{z} : z_1 z_2 z'_3 \equiv 0\}$ .

Begin by placing a lower bound on the acceptance probability  $\Pr[\text{accept}]$  conditioned on acceptance of both  $X$ -error verifications. As in the  $X$ -error verification component, we use an estimate based on the good events only:

$$\begin{aligned}
\Pr[\text{accept}|\text{accept}^{(1,2)}] &\geq \Pr[\text{accept}, \text{good}_Z|\text{accept}^{(1,2)}] \\
&= 1 - \Pr[\neg \text{accept}, \text{good}_Z|\text{accept}^{(1,2)}] - \Pr[\text{bad}_Z|\text{accept}^{(1,2)}] \\
\Pr[\neg \text{accept}, \text{good}_Z|\text{accept}^{(1,2)}] &= \sum_{\substack{\vec{z} \notin \text{accept}_Z \\ |\vec{k}| \leq 7}} \left( \Pr[\zeta_3 = z_3, K_{Z,3} = k_3, \text{good}_Z^{(3)}] \cdot \prod_{j=1}^2 \Pr[\zeta_j = z_j, K_{Z,j} = k_j, \text{good}_Z^{(j)}|\text{accept}^{(j)}] \right) \quad (\text{A.13}) \\
&\leq \sum_{\substack{\vec{z} \notin \text{accept}_Z \\ |\vec{k}| \leq 7}} \Pr[\zeta_3 = z_3, K_{Z,3} = k_3, \text{good}_Z^{(3)}] \prod_{j=1}^2 \frac{\mathcal{P}_j(z_j, k_j)}{\Pr[\text{accept}^{(j)}]},
\end{aligned}$$

where  $\mathcal{P}_j$  is defined according to (A.10).

Now consider  $Z$  errors, the simpler case. We have

$$\Pr[\zeta = z, K_Z \leq k, \text{good}_Z, \text{accept} | \text{accept}^{(1,2)}] \leq \sum_{\substack{\vec{z} \in \text{out}(z) \cap \text{accept}_Z \\ |\vec{k}| \leq \min\{k, 7\}}} \left( \frac{\Pr[\zeta_3 = z_3, K_{Z,3} = k_3, \text{good}_Z^{(3)}]}{\prod_{j=1}^2 \frac{\mathcal{P}_j(z_j, k_j)}{\Pr[\text{accept}^{(j)}]}} \right). \quad (\text{A.14})$$

We upper-bound  $\Pr[\zeta = z, K_Z \leq k, \text{good}_Z | \text{accept}, \text{accept}^{(1,2)}]$  by the minimum of one and the ratio of  $\Pr[\zeta = z, K_Z \leq k, \text{good}_Z, \text{accept} | \text{accept}^{(1,2)}]$  divided by the previously computed lower bound on  $\Pr[\text{accept} | \text{accept}^{(1,2)}]$ .

Next consider  $X$  errors. Under the  $X$ -only noise model, we have no information about  $Z$  errors and we must pessimistically assume that all  $X$  errors pass verification (i.e.,  $\Pr[\chi, \text{accept}] = \Pr[\chi]$ ). In reality, some of the  $X$  errors will occur with  $Z$  errors and will be rejected. In the same way that corrections were applied for  $Z$ -error counts during  $X$ -error verification, we apply low-order corrections to the  $X$ -error counts by considering  $X$  and  $Z$  errors together. In a similar manner to Eq. (A.8) we have

$$\begin{aligned} \Pr[\chi = x, \text{good}_X, \text{accept} | \text{accept}^{(1,2)}] \\ \leq \frac{\Pr[\chi = x, \text{good}_X, \text{accept}^{(1,2)}] - \Pr[\chi = x, \text{best}, \neg \text{accept}, \text{accept}^{(1,2)}]}{\Pr[\text{accept}^{(1)}] \Pr[\text{accept}^{(2)}]}. \end{aligned} \quad (\text{A.15})$$

The numerator terms on the right-hand side can be computed as

$$\Pr[\chi = x, \text{good}_X, \text{accept}^{(1,2)}] = \sum_{\substack{\vec{x} \in \text{out}(x) \\ |\vec{k}| \leq 7}} \prod_{j=1}^3 \Pr[\chi_j = x_j, K_{X,j} = k_j, \text{good}_X^{(j)}, \text{accept}^{(j)}] \quad (\text{A.16})$$

$$\begin{aligned} \Pr[(\chi, \zeta) = (x, z), \text{best}, \neg \text{accept}, \text{accept}^{(1,2)}] = \\ \sum_{\substack{\vec{z} \in \text{out}(z) \setminus \text{accept}_Z \\ \vec{x} \in \text{out}(x), |\vec{k}| \leq 1}} \prod_{j=1}^3 \Pr[(\chi_j, \zeta_j) = (x_j, z_j), K_j = k_j, \text{accept}^{(j)}]. \end{aligned} \quad (\text{A.17})$$

Equation (A.15) is then upper bounded by upper bounding (A.16), lower bounding  $\Pr[\text{accept}^{(1)}]$  and  $\Pr[\text{accept}^{(2)}]$ , and computing (A.17) with equality, all of which can be accomplished with quantities from Appendix A.2.

This correction is less significant than the similar correction applied in  $X$ -error verification. By the time  $Z$ -error verification occurs, many of the  $X$ -errors have already been eliminated by  $X$ -error verification. The  $X$  errors that do pass verification are less correlated with  $Z$  errors; the correction eliminates only about 39 percent of the nontrivial  $X$  errors compared to about 57 percent for the analogous  $X$ -error verification correction. Furthermore, this correction has no effect on normalization because acceptance at this stage depends only on  $Z$  errors, and there are no further postselection steps in the exRec.

#### A.4 Error correction

The error correction component (Figure 14) contains four independent sub-components. The  $\text{bad}_X$  events for sub-components one and two are defined in Appendix A.3. The  $\text{bad}_X$  event for sub-

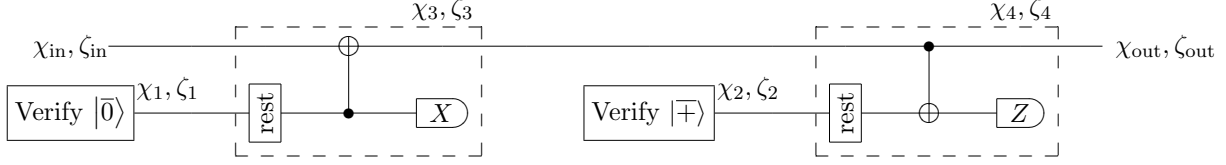


Figure 14: The error correction component. Error correction consists of a  $Z$ -error correction followed by an  $X$ -error correction. The  $Z$ -error correction requires a verified encoded  $|\bar{0}\rangle$  ancilla and the  $X$ -error correction requires a verified encoded  $|\bar{+}\rangle$  ancilla.

components three and four occur when there are more than four failures inside of the sub-component. Define the error correction component to be  $\text{bad}_X$  if any of the sub-components are  $\text{bad}_X$  or there are more than eleven  $X$  failures total. Similarly define  $\text{bad}_Z$  for  $Z$  failures.

All events are conditioned on the successful verification of both the  $|\bar{0}\rangle$  and  $|\bar{+}\rangle$  ancillas. We have

$$\Pr[\text{bad}_X | \text{accept}^{(1,2)}] \leq \sum_{j=1}^2 \Pr[\text{bad}_X^{(j)} | \text{accept}^{(j)}] + \sum_{j=3}^4 \Pr[\text{bad}_X^{(j)}] + \Pr[K_X > 11] . \quad (\text{A.18})$$

Here,  $\text{accept}^{(j)}$  means that *all* verification tests,  $X$  and  $Z$ , within that subcomponent have passed.

Consider first  $X$  errors. For the two leading error corrections, we are concerned only with the case in which the incoming error syndrome is zero. Nonzero syndromes on the input may result in a (undetectable) logical error at the output. However, as noted in [Section 4.3.4](#), this has no impact on either the output syndrome or the correctness of the 1-Rec. The probability of an  $X$  error  $x$  at the output is expressed as  $\Pr[\chi_{\text{out}} = x, \text{good} | \chi_{\text{in}} \equiv 0]$ .

For the two trailing error corrections, we must consider all possible inequivalent errors on the input. However, we do not need to compute the probability of each individual error at the output. Rather, we care only about the the probability of an uncorrectable error. Let  $\mathcal{E}$  be the set of correctable errors on a single block and  $\bar{\mathcal{E}}$  be the set of uncorrectable errors, and for an error  $e$ , let

$$D(e) = \begin{cases} 1 & \text{if } e \in \bar{\mathcal{E}} \\ 0 & \text{if } e \in \mathcal{E} \end{cases} . \quad (\text{A.19})$$

We use, for  $d \in \{0, 1\}$ ,

$$\Pr[D(\chi_{\text{out}}) = d, \text{good}_X | \chi_{\text{in}} = x_{\text{in}}] \leq \sum_{x: D(x)=d} \Pr[\chi_{\text{out}} = x, \text{good}_X | \chi_{\text{in}} = x_{\text{in}}] . \quad (\text{A.20})$$

The terms of the sum may be expanded as usual by partitioning  $k$  failures among the sub-components of the EC. Define  $\text{out}(x) := \{\vec{x} : x_{\text{in}} x_1 x'_3 x'_4 \text{Corr}(x_{\text{in}} x_1 x_2 x'_3 x''_4) \equiv x\}$ , where  $\text{Corr}(\cdot)$  gives the classically computed correction for the syndrome of its argument. Then

$$\Pr[\chi_{\text{out}} = x, K_X \leq k, \text{good}_X | \chi_{\text{in}} = x_{\text{in}}] = \sum_{\substack{\vec{x} \in \text{out}(x) \\ |\vec{k}| \leq 11}} \prod_{j=1}^4 \Pr[\chi_j = x_j, K_{X,j} = k_j, \text{good}_X^{(j)}] , \quad (\text{A.21})$$

which can be upper bounded using quantities from [Appendix A.3](#). Calculations for  $Z$  errors are analogous except using  $\text{out}(z) := \{\vec{z} : z_{\text{in}} z_2 z'_3 z'_4 \text{Corr}(z_{\text{in}} z_1 z'_3) \equiv z\}$ .

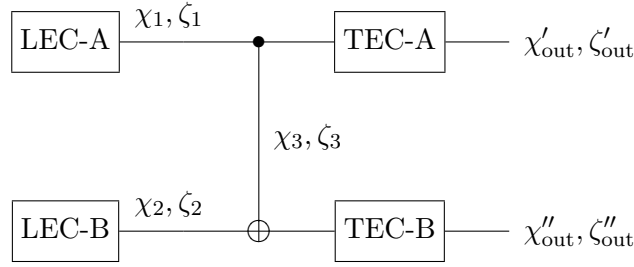


Figure 15: The CNOT exRec consists of two leading error corrections, a transversal CNOT with controls on block A and targets on block B, and two trailing error corrections. Incremental errors for the LECs and the CNOT are labeled, as are the total errors at the output of each block.

## A.5 exRec

The exRec is divided into five sub-components: the leading error correction on block A (LEC-A), the leading error correction on block B (LEC-B), the transversal CNOT from block A to block B, the trailing error correction on block A (TEC-A) and the trailing error correction on block B (TEC-B). See Figure 15.

The  $\text{bad}_X$  event for the error correction sub-components is defined in Appendix A.4. The  $\text{bad}_X$  event for the transversal CNOT occurs when it contains more than two  $X$  failures. The  $\text{bad}_X$  event for the exRec (and analogously the  $\text{bad}_Z$  event) occurs when any of the following are true:

- Any of the sub-components are  $\text{bad}_X$ .
- There are more than 25  $X$  failures in the exRec.
- There is more than one  $X$  failure in the transversal CNOT *and* there are more than three  $X$  failures in each of the two leading ECs.

The last condition eliminates faults that are particularly difficult to count. The time required to count an exRec fault is proportional to the product of the number of unique syndromes that can result at the output of the two leading ECs and the transversal CNOT. The number of unique syndromes that can result from the transversal CNOT with two  $X$  failures is  $\binom{23}{2} 3^2 = 2277$ , while the number of unique syndromes with one  $X$  failure is  $23 \cdot 3 = 69$ . The numbers of unique syndromes at the output of the leading ECs are 24, 277 and 2048 for one, two, and three  $X$  failures respectively. So, for example, the event  $K_{X,1} = 2, K_{X,2} = 3, K_{X,3} = 1$  ( $277 \cdot 2048 \cdot 69 \approx 4 \cdot 10^7$ ) requires far less time than the event  $K_{X,1} = 2, K_{X,2} = 3, K_{X,3} = 2$  ( $277 \cdot 2048 \cdot 2277 \approx 1 \cdot 10^9$ ). In particular, we would like to avoid counting faults for which  $K_{X,3} = 2$ .

The probability of the  $\text{bad}_X$  event, conditioned on acceptance of all  $X$ -error and  $Z$ -error verifications is

$$\begin{aligned} \Pr[\text{bad}_X | \text{accept}^{(1,2,4,5)}] &\leq \sum_{j \in \{1,2,4,5\}} \Pr[\text{bad}_X^{(j)} | \text{accept}^{(j)}] + \Pr[\text{bad}_X^{(3)}] \\ &\quad + \Pr[K_X > 25] + \Pr[K_{X,3} > 1] \prod_{j=1}^2 \Pr[K_{X,j} > 3 | \text{accept}^{(j)}] . \end{aligned} \tag{A.22}$$

Computed upper bounds for this quantity are plotted in Figure 16(b). Naïvely one might expect bounds for partial exRecs—those for which one or more TECs have been removed—to be lower than bound for the full exRec by as much as a factor of two. However, (A.22) is dominated by either the transversal CNOT ( $\Pr[\text{bad}_X^{(3)}]$ ) or the condition involving the transversal CNOT and the two LECs ( $\Pr[K_{X,3} > 1] \prod_{j=1}^2 \Pr[K_{X,j} > 3 | \text{accept}^{(j)}]$ ) over most of the domain of  $p$ . Thus removing the TECs has little impact on the probability that the exRec is bad.

Recall from (A.19) the definition of  $D : (\mathcal{E} \cup \bar{\mathcal{E}}) \rightarrow \{0, 1\}$ . For  $\vec{x} = (x_1, x_2, x_3, x'_{\text{out}}, x''_{\text{out}})$  and  $\vec{z} = (z_1, z_2, z_3, z'_{\text{out}}, z''_{\text{out}})$ , we can then define the malignant  $X$ - and  $Z$ -error events for the CNOT 1-Rec as

$$\begin{aligned} \text{mal}_{IX}(\vec{x}) &:= [D(x_1) = D(x'_{\text{out}})] \wedge [D(x_1) \oplus D(x_2) \neq D(x''_{\text{out}})] \\ \text{mal}_{XI}(\vec{x}) &:= [D(x_1) \neq D(x'_{\text{out}})] \wedge [D(x_1) \oplus D(x_2) = D(x''_{\text{out}})] \\ \text{mal}_{XX}(\vec{x}) &:= [D(x_1) \neq D(x'_{\text{out}})] \wedge [D(x_1) \oplus D(x_2) \neq D(x''_{\text{out}})] \\ \text{mal}_{IZ}(\vec{z}) &:= [D(z_1) \oplus D(z_2) = D(z'_{\text{out}})] \wedge [D(z_2) \neq D(z''_{\text{out}})] \\ \text{mal}_{ZI}(\vec{z}) &:= [D(z_1) \oplus D(z_2) \neq D(z'_{\text{out}})] \wedge [D(z_2) = D(z''_{\text{out}})] \\ \text{mal}_{ZZ}(\vec{z}) &:= [D(z_1) \oplus D(z_2) \neq D(z'_{\text{out}})] \wedge [D(z_2) \neq D(z''_{\text{out}})] \quad . \end{aligned} \tag{A.23}$$

These are the events for which the behavior of the 1-Rec differs from the behavior of an ideal decoder followed by an ideal (level-zero) CNOT gate, i.e., the 1-Rec is incorrect. The subscripts denote the logical error introduced by the exRec. For example,  $\text{mal}_{IX}$  is the event in which the action of the exRec followed by an ideal decoder is the same as that of an ideal decoder followed by an ideal CNOT gate plus the two-qubit error  $I \otimes X$ .

For each error event  $E \in \{IX, XI, XX\}$ , we are interested in the probability that  $\text{mal}_E(\vec{\chi})$  occurs along with the  $\text{good}_X$  event. Define  $G := \{\vec{k} : |\vec{k}| \leq 25, k_3 \leq 1 \text{ if } k_1 \geq 4 \text{ and } k_2 \geq 4\}$ . Then, letting  $\chi'_{\text{in}}$  and  $\chi''_{\text{in}}$  be the errors input to the two TECs,

$$\Pr[\text{mal}_E(\vec{\chi}), \text{good}_X] = \sum_{\substack{\vec{x}: \text{mal}_E(\vec{x}) \\ \vec{k} \in G}} \left[ \prod_{j=1}^3 \Pr[\chi_j = x_j, K_{X,j} = k_j, \text{good}_X^{(j)}] \cdot \Pr[\chi'_{\text{out}} = x'_{\text{out}}, K_{X,4} = k_4, \text{good}_X^{(4)} | \chi'_{\text{in}} \equiv x_1 x'_3] \cdot \Pr[\chi''_{\text{out}} = x''_{\text{out}}, K_{X,5} = k_5, \text{good}_X^{(5)} | \chi''_{\text{in}} \equiv x_1 x_2 x''_3] \right], \tag{A.24}$$

which may be upper bounded using quantities from Appendix A.4. Calculation of  $\Pr[\text{mal}_E(\vec{\zeta}), \text{good}_Z]$  for  $E \in \{IZ, ZI, ZZ\}$  is analogous.

## B Implementation of component counting

Equations (A.22) and (A.24) in Appendix A are conceptually straightforward and easy to compute numerically for a fixed  $\gamma$ . However, we would like to compute exact bounds that hold for a range of  $\gamma$ . In this appendix, we will specify a few of the implementation details that allow for maintaining the bounds as polynomials with integer coefficients.

The ultimate goal is to compute upper bounds on the probabilities of malignant events at the outermost layer of the exRec. That is, we want to compute (A.22), (A.24) and combine them to get

$$\Pr[\text{mal}_E(\vec{\chi}) | \text{accept}] \leq \Pr[\text{mal}_E(\vec{\chi}), \text{good}_X | \text{accept}] + \Pr[\text{bad}_X | \text{accept}] \quad . \tag{B.1}$$

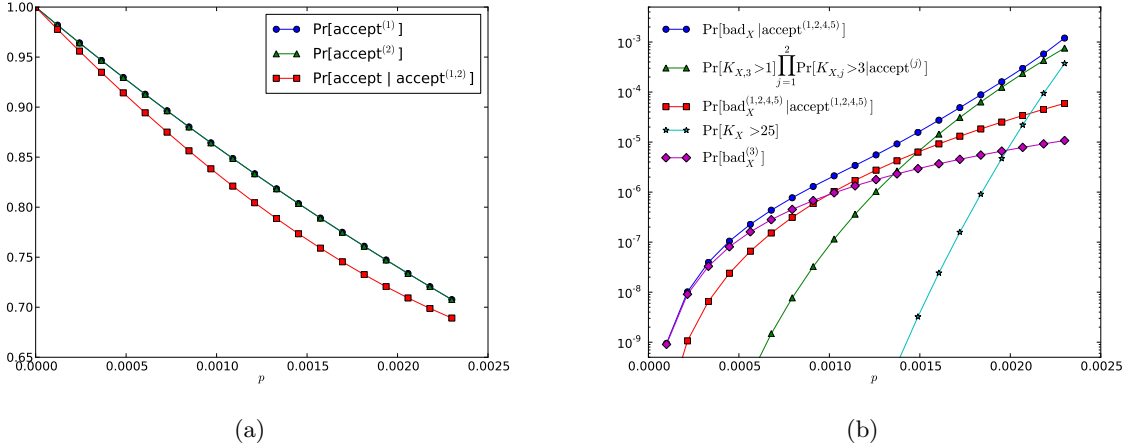


Figure 16: Plotted in (a) are lower bounds on the Overlap-4 acceptance probabilities for the two  $X$ -error verifications ( $\text{accept}^{(1)}$  and  $\text{accept}^{(2)}$ ) and for the  $Z$ -error verification ( $\text{accept}$ ) conditioned on success of the  $X$ -error verifications. The plot in (b) shows upper bounds on (A.22), the probability that the CNOT exRec is bad.

The right-hand side of this inequality decomposes into sums of individual component quantities of the form

$$\Pr[\chi = x, K_X = k] = \sum_{|\vec{k}|=k} \Pr[\chi = x, \vec{K}_X = \vec{k}] , \quad (\text{B.2})$$

where  $\vec{k} = (k_c, k_r, k_p, k_m)$  expresses the number of failing CNOT, rest,  $|0\rangle$  preparation and  $Z$ -basis measurements, respectively.

For each term in the sum, the number of failures for each type of location is fixed, but the particular locations on which those failures occur are not fixed, nor are the errors that occur at those locations. Let  $L(\vec{k}) := \{(\vec{l}_c, \vec{l}_r, \vec{l}_p, \vec{l}_m) : (|\vec{l}_c|, |\vec{l}_r|, |\vec{l}_p|, |\vec{l}_m|) = \vec{k}\}$  be the set of all possible tuples of failing locations consistent with  $\vec{k}$ . Also, let  $E(\vec{l})$  be the set of all possible tuples of  $X$  errors consistent with failures at locations  $\vec{l}$ . To fix the locations and the errors, use

$$\begin{aligned} \Pr[\chi = x, \vec{K}_X = \vec{k}] &= \sum_{\vec{l} \in L(\vec{k}), \vec{e} \in E(\vec{l})} \Pr[\chi = x, \vec{E} = \vec{e}] \\ &= \sum_{\vec{l} \in L(\vec{k}), \vec{e} \in E(\vec{l})} \mathcal{F}(x, \vec{e}) \Pr[\vec{E} = \vec{e}] \end{aligned} \quad (\text{B.3})$$

where in the second line we have made the substitution  $\mathcal{F}(x, \vec{e}) = \Pr[\chi = x | \vec{E} = \vec{e}]$ .

The boolean function  $\mathcal{F}(x, \vec{e})$  takes value one if the component produces the error  $x$  for a given “configuration” of errors  $\vec{e}$  and value zero otherwise. The error configuration  $\vec{e}$  fully specifies the the locations that have failed and the error at each failing location. Let  $n_c, n_r, n_p, n_m$  be the total number of CNOT, rest,  $|0\rangle$  preparations and  $Z$ -basis measurements in the component, respectively.



Then from the marginal noise model discussed in [Section 4.1](#) we have

$$\begin{aligned} \Pr[\vec{E} = \vec{e}] &= (1 - 4\gamma)^{n_p + n_m} (1 - 8\gamma)^{n_r} (1 - 12\gamma)^{n_c} \left(\frac{4\gamma}{1 - 4\gamma}\right)^{k_p + k_m} \left(\frac{8\gamma}{1 - 8\gamma}\right)^{k_r} \left(\frac{4\gamma}{1 - 12\gamma}\right)^{k_c} \\ &\leq A_{\vec{n}} 4^k 2^{k_r} \left(\frac{\gamma}{1 - 12\gamma}\right)^k, \end{aligned} \quad (\text{B.4})$$

where  $A_{\vec{n}}$  is defined as in [\(A.1\)](#). This inequality is a reasonable approximation for the range  $\gamma \leq \frac{2 \times 10^{-3}}{15}$  with which we are concerned. It allows us to move  $\gamma$  into a prefactor in front of the sum of [\(B.2\)](#), and permits an integer representation in the computer analysis. Indeed, substituting back into equation [\(B.2\)](#) gives

$$\Pr[\chi = x, K_X = k] \leq A_{\vec{n}} \left(\frac{\gamma}{1 - 12\gamma}\right)^k \sum_{\substack{|\vec{k}|=k \\ \vec{l} \in L(\vec{k}), \vec{e} \in E(\vec{l})}} 4^k 2^{k_r} \mathcal{F}(x, \vec{e}). \quad (\text{B.5})$$

$X$ - and  $Z$ -error verification require corrections that involve counting  $X$  and  $Z$  errors together ([Appendix A.2](#)). In that case, the probability of an error configuration is computed according to [Definition 4.1](#) and we require a lower bound. We have

$$\begin{aligned} \Pr[\vec{E} = \vec{e}] &= (1 - 4\gamma)^{n'_p + n'_m} (1 - 12\gamma)^{n_r} (1 - 15\gamma)^{n_c} \left(\frac{4\gamma}{1 - 4\gamma}\right)^{k_p + k_m} \left(\frac{4\gamma}{1 - 12\gamma}\right)^{k_r} \left(\frac{\gamma}{1 - 15\gamma}\right)^{k_c} \\ &\geq A'(\vec{n}') 4^{k_p + k_m + k_r} \left(\frac{\gamma}{1 - 4\gamma}\right)^k \\ &= A_{\vec{n}} \left(\frac{A'(\vec{n}')}{A_{\vec{n}}}\right) \left(\frac{\gamma}{1 - 12\gamma}\right)^k \left(\frac{1 - 12\gamma}{1 - 4\gamma}\right)^k 4^{k_p + k_m + k_r} \\ &\geq A_{\vec{n}} \left(\frac{\gamma}{1 - 12\gamma}\right)^k \mathcal{S} 4^{k_p + k_m + k_r}. \end{aligned} \quad (\text{B.6})$$

Here,  $n'_p$  and  $n'_m$  are the total numbers of preparation and measurement locations (including now  $|+\rangle$  preparations and  $X$ -basis measurements), and  $A'(\vec{n}') = (1 - 4\gamma)^{n'_p + n'_m} (1 - 12\gamma)^{n_r} (1 - 15\gamma)^{n_c}$ . The scaling factor  $\mathcal{S} = \lfloor \frac{A'(\vec{n}')}{A_{\vec{n}}} \left(\frac{1 - 12\gamma_{\max}}{1 - 4\gamma_{\max}}\right)^k \rfloor$  converts the  $XZ$  probability into a form that is compatible with  $X$ -only and  $Z$ -only probabilities (Eq. [\(B.4\)](#)) while maintaining the lower bound and integer representation. The constant  $\gamma_{\max}$  is chosen so that it is higher than the expected threshold value. Now, [\(A.8\)](#) and [\(A.15\)](#) can be rewritten so that the sums do not depend on  $\gamma$ , and terms with corrections such as [\(A.10\)](#) can be represented by a single integer.

Another advantage of counting component probabilities as likelihoods, is that the counts compose nicely. If we apply [\(B.2\)](#) to itself and combine with [\(B.5\)](#), we end up with

$$\begin{aligned} \Pr[\chi = x, K_X = k] &= \sum_{\substack{|\vec{k}|=k \\ \vec{x} \in \text{out}(x)}} \prod_j \Pr[\chi_j = x_j, K_{X,j} = k_j] \\ &\leq A_{\vec{n}} \left(\frac{\gamma}{1 - 12\gamma}\right)^k \left[ \sum_{\substack{|\vec{k}|=k \\ \vec{x} \in \text{out}(x)}} \prod_j \sum_{\substack{|\vec{k}_j|=k_j \\ \vec{l} \in L(\vec{k}_j), \vec{e} \in E(\vec{l})}} 4^{k_j} 2^{k_{j,r}} \mathcal{F}(x_j, \vec{e}) \right]. \end{aligned} \quad (\text{B.7})$$

The substitution made in the first line can be applied successively for each sub-component  $j$ . Once the lowest level component is reached, we use (B.5) to push dependence on  $\gamma$  outside of the sum. The integer value inside of the brackets is the discrete convolution of weighted counts from the sub-components summed over all possible failure partitions  $\vec{k}$  of size  $k$ . It is a weighted count of all possible ways to produce error  $x$  with an order  $k$  fault.

The primary task of the Python program is to compute  $\mathcal{F}$  for each (good) error configuration, starting with the lowest level component, and to store the resulting weighted sums

$$\sum_{\substack{|\vec{k}|=k \\ \vec{l} \in L(\vec{k}), \vec{e} \in E(\vec{l})}} 4^k 2^{k_r} \mathcal{F}(x, \vec{e}) \quad (\text{B.8})$$

(or equivalent) for use in the counting for larger components. At each level, counts for the sub-components are convolved to generate new counts. The prefactor  $A_{\vec{n}} \left( \frac{\gamma}{1-12\gamma} \right)^k$  need only be computed at the end, when calculating the threshold.

## C Monotonicity of malignant event upper bounds

We now show how to prove that the level-one malignant event polynomials constructed by our counting method are monotone non-decreasing over the interval  $\gamma \in [0, 1.8 \times 10^{-3}]$ , which encompasses our threshold values. Monotonicity of level-one upper bounds is not strictly required for the proof of Theorem 4.3. However, it is useful constructing the transformed noise model (see Appendix D.2) and in finding the maximum  $\gamma$  that satisfies  $\mathcal{P}_E^{(2)}(\Gamma^{(1)}) \leq \alpha_E \Gamma^{(1)}$ . Monotonicity of upper bounds for level-two and above follow from Claim 4.2 which depends only on the construction defined by our counting method and not on the actual counting results—see Appendix D.3. Level-one polynomials, however, can include terms that decrease with  $\gamma$ . Monotonicity statements for level-one bounds, therefore, depend on coefficients—i.e., weighted counts—computed by our Python implementation.

Recall that the upper bound  $\mathcal{P}_E$  for malignant event  $\text{mal}_E$  as defined by Appendix A is of the form

$$\mathcal{P}_E \geq \frac{\Pr[\text{mal}_E, \text{good}]}{\Pr[\text{accept}]} + \Pr[\text{bad}|\text{accept}] \quad (\text{C.1})$$

Consider first the  $\Pr[\text{bad}|\text{accept}]$  term. This term is expressed as sums and products of  $\Pr[\text{bad}]$  terms, some of which contain  $\Pr[\text{accept}]$  terms in the denominator. The  $\Pr[\text{bad}]$  and  $\Pr[\text{accept}]$  terms are, in turn, expressed as sums and products of polynomials  $\mathcal{Q}$  of the form

$$\mathcal{Q}(\gamma) = A_{\vec{n}}(\gamma) \sum_{k=k_{\min}}^{k_{\max}} c(k) \left( \frac{\gamma}{1-12\gamma} \right)^k, \quad (\text{C.2})$$

where  $\mathcal{Q}(\gamma) \geq 0$  for all  $\gamma \geq 0$ , and integer coefficients  $c(k)$  do not depend on  $\gamma$ . The quantity  $\Pr[\text{mal}_E, \text{good}]$  is also expressed in this way. Our goal then is to use (C.2) to show that  $\Pr[\text{accept}]$  is monotone non-increasing, and that  $\Pr[\text{bad}]$  and  $\Pr[\text{mal}_E, \text{good}]/\Pr[\text{accept}]$  are monotone non-decreasing over the desired range. Note that  $\Pr[\text{mal}_E, \text{good}]$  is, in fact, not monotone over our chosen range.

The derivative of  $\mathcal{Q}$  is a sum of two terms. The first term can be lower-bounded by using

$$\begin{aligned} \frac{dA_{\vec{n}}}{d\gamma} \sum_{k=k_{\min}}^{k_{\max}} c(k) \left( \frac{\gamma}{1-12\gamma} \right)^k &= \left( \frac{-12n_c}{1-12\gamma} - \frac{8n_r}{1-8\gamma} - \frac{4n_{pm}}{1-4\gamma} \right) A_{\vec{n}} \sum_k c(k) \left( \frac{\gamma}{1-12\gamma} \right)^k \\ &\geq -(12n_c + 8n_r + 4n_{pm}) \frac{\mathcal{Q}(\gamma)}{1-12\gamma} . \end{aligned} \quad (\text{C.3})$$

If all coefficients  $c(k)$  are non-negative, then the second term may be lower-bounded as

$$A_{\vec{n}} \sum_k c(k) \frac{d}{d\gamma} \left( \frac{\gamma}{1-12\gamma} \right)^k \geq \frac{k_{\min}}{\gamma_{\max}} \frac{\mathcal{Q}(\gamma)}{1-12\gamma} . \quad (\text{C.4})$$

In the case of  $\text{Pr}[\text{bad}]$ , all of the coefficients  $c(k)$  are, indeed, non-negative. Using  $\gamma_{\min} = 0$ , and  $k_{\min} = k_{\text{good}} + 1$  we obtain

$$\frac{d \text{Pr}[\text{bad}]}{d\gamma} \geq \left( \frac{k_{\text{good}} + 1}{\gamma_{\max}} - 12n_c - 8n_r - 4n_{pm} \right) \frac{\text{Pr}[\text{bad}]}{1-12\gamma} , \quad (\text{C.5})$$

which is non-negative over  $[0, 1.8 \times 10^{-3}]$  for all of our components.

We would like to upper bound the denominator quantities  $\text{Pr}[\text{accept}]$  using a condition analogous to (C.5). Such a condition is insufficient, however, because for  $X$ -error verification  $k_{\min} = 0$ , and for  $Z$ -error verification some coefficients may be negative due to low-order  $XZ$  corrections. Instead, we bound the second derivative using the following inequality due to Markov.

**Lemma C.1** (see, e.g., [Haz90] pp. 100). *Let  $\mathcal{Q}$  be a univariate polynomial of degree at most  $n$ . Then the  $m$ -th order derivative  $\mathcal{Q}^{(m)}$  is bounded by*

$$\max_{\gamma \in [\gamma_{\min}, \gamma_{\max}]} |\mathcal{Q}^{(m)}(\gamma)| \leq \frac{2^m \prod_{k=0}^{m-1} (n^2 - k^2)}{(\gamma_{\max} - \gamma_{\min})^m (2m-1)!!} \max_{\gamma \in [\gamma_{\min}, \gamma_{\max}]} |\mathcal{Q}(\gamma)| . \quad (\text{C.6})$$

In our case,  $n$  is bounded by the number of locations in the corresponding component. The maximum of  $\mathcal{Q}$  is obtained by separating the positive and negative coefficients and upper bounding by

$$\max_{\gamma \in [\gamma_{\min}, \gamma_{\max}]} \mathcal{Q}(\gamma) \leq A_{\vec{n}}(\gamma) \sum_{k=k_{\min}}^{k_{\max}} \frac{\max\{c(k), 0\} \gamma_{\max}^k}{(1-12\gamma_{\max})^k} + \frac{\min\{c(k), 0\} \gamma_{\min}^k}{(1-12\gamma_{\min})^k} . \quad (\text{C.7})$$

If  $\Delta$  is the bound obtained from Lemma C.1, then the first derivative can be bounded using

$$\max_{\gamma \in [\gamma_{\min}, \gamma_{\max}]} \mathcal{Q}^{(1)} \leq \mathcal{Q}^{(1)}(\gamma_{\min}) + \Delta(\gamma_{\max} - \gamma_{\min}) . \quad (\text{C.8})$$

Depending on the values of the coefficients  $c(k)$ , bounding the first derivative below zero may require dividing up the interval into smaller sub-intervals and successively applying (C.8).

Analysis for  $\mathcal{Q} = \text{Pr}[\text{mal}_E, \text{good}] / \text{Pr}[\text{accept}]$  is similar. Monotonicity over the range  $[\epsilon, \gamma_{\max}]$  for small constant  $\epsilon$  can be shown by using the lower bound equivalent of (C.8). The maximum of  $\mathcal{Q}$  is calculated by using (C.7) on  $\text{Pr}[\text{mal}_E, \text{good}]$  and evaluating  $\text{Pr}[\text{accept}]$  at  $\gamma_{\max}$ . Lower bounding the first derivative in this way is not adequate for  $[0, \epsilon]$ , however, because the first derivative vanishes at  $\gamma = 0$ . Due to the strict fault-tolerance of our circuits, coefficients  $c(k)$  of  $\text{Pr}[\text{mal}_E, \text{good}]$  are zero for  $0 \leq k \leq 3$  and so the derivatives up to third order are also zero. To show monotonicity over  $[0, \epsilon]$  we evaluate the fourth derivative at  $\gamma = 0$  and then use Lemma C.1 to bound the fifth derivative.

## D The transformed noise model

### D.1 Construction of the model

The transformed noise model uses upper bounds on the level-one malignant event probabilities to model each 1-Rec as a single effective “location” in the level-two simulation. The construction here considers only  $X$ -error malignant events. Construction for  $Z$ -error events is nearly identical, and the upper bounds obtained from level-one counting contain no information about  $X$  and  $Z$  correlations so  $X$  and  $Z$  errors are not considered together at level-two.

From level-one counting, we have upper bounds on  $\Pr[\text{mal}_{IX}]$ ,  $\Pr[\text{mal}_{XI}]$ , and  $\Pr[\text{mal}_{XX}]$  of the transversal CNOT,  $\Pr[\text{mal}_X^{\text{prep}}]$  of encoded  $|0\rangle$  preparation,  $\Pr[\text{mal}_X^{\text{meas}}]$  of transversal  $Z$ -basis measurement and  $\Pr[\text{mal}_X^{\text{rest}}]$  of the transversal rest. Each of these bounds is a polynomial in  $\gamma$ , the probability of a given error on a physical CNOT (see Figure 11(a)). Denote the upper bound polynomial for each event  $\text{mal}_E$  by  $\mathcal{P}_E$ . Then let  $\Gamma_X(\gamma)$  be a polynomial defined over the interval  $0 \leq \gamma \leq \gamma_{\max}$  such that, for all  $\text{mal}_E$ ,

$$\mathcal{P}_E(\gamma) \leq \alpha_E \Gamma_X(\gamma) \quad (\text{D.1})$$

where  $\alpha_E \geq 1$  is a constant. The procedure for obtaining such a polynomial  $\Gamma_X$  and constants  $\alpha_E$  is outlined in the Section D.2.

Now consider the level-two simulation. Level-two rectangles are composed of many level-one rectangles. Following [AGP06] we replace each 1-Rec with an implementation of the corresponding (level-zero) gate, starting with the right-most 1-Recs and moving left. If a 1-Rec is correct, then it is replaced with an ideal gate. If a 1-Rec is incorrect, then the entire exRec is replaced with a faulty version of the gate. Unlike [AGP06], however, exRecs containing incorrect rectangles are replaced according to the malignant event that occurred. For example, a CNOT 1-Rec that is  $\text{mal}_{IX}$  is replaced with an ideal CNOT gate followed by the error  $I \otimes X$ . A 1-Rec ( $A$ ) that precedes an incorrect 1-Rec ( $B$ ) is replaced with a faulty gate only if  $A$  is still incorrect after the ECs shared with the exRec containing  $B$  have been removed. Such an incorrect 1-Rec ( $A$ ) is said to be “independently” incorrect.

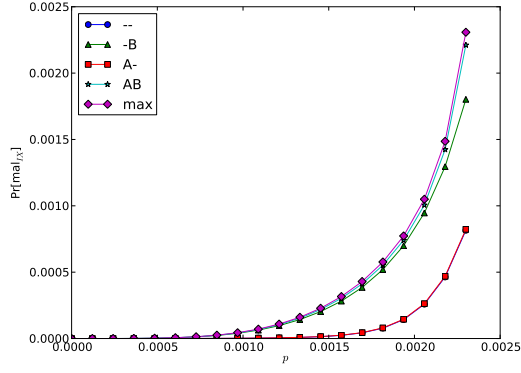
Let  $K_1, K_2, K_3, K_4, K_5$  be the number of level-one exRecs that are independently  $\text{mal}_{IX}$ ,  $\text{mal}_{XI}$ ,  $\text{mal}_{XX}$ ,  $\text{mal}_X^{\text{prep}}$ ,  $\text{mal}_X^{\text{meas}}$  and  $\text{mal}_X^{\text{rest}}$ , respectively. Then the probability  $\Pr[\vec{K} = \vec{k}]$  of this event is bounded by

$$\Pr[\vec{K} = \vec{k}] \leq \Gamma_X(\gamma)^{|\vec{k}|} \prod_{i=1}^6 \lceil \alpha_i \rceil^{k_i} \quad (\text{D.2})$$

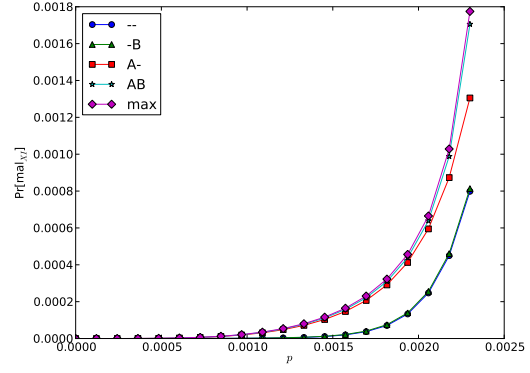
where the ceiling is taken to allow integer representation in the computer analysis. Thus, characterization and analysis of the level-two components is similar to that used for the depolarizing noise model in Section A except that the weights associated with each type of error are different. There is also no prefactor  $A_{\vec{n}}$  in (D.2) as there is in (B.4). This is because the error probabilities are now specified as upper bounds rather than equalities. We do not have a proper upper bound, other than one, for the probability that a location (1-Rec) does *not* fail.

### D.2 Bounding malignant event polynomials

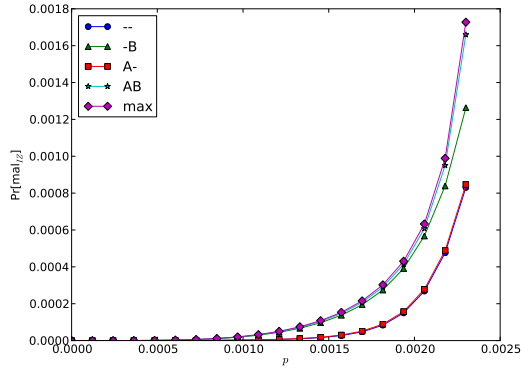
Construction of the transformed noise model requires bounding of several sets of polynomials in two different ways. The first case compares polynomials of a fixed malignant event for each possible



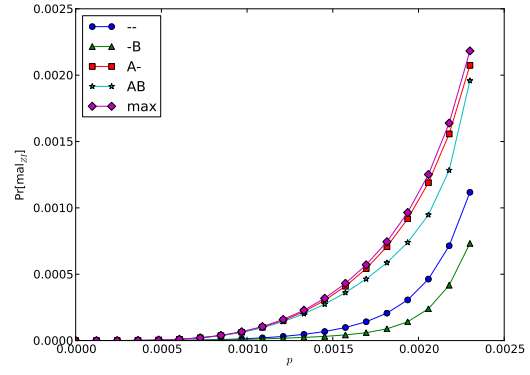
(a)



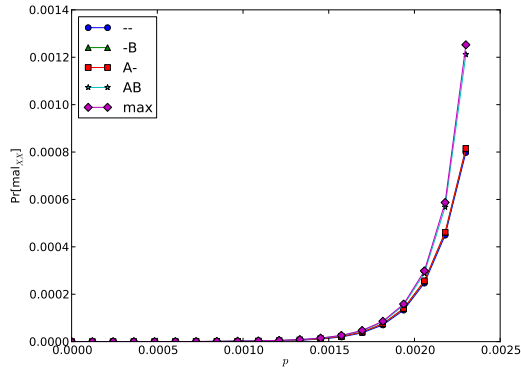
(b)



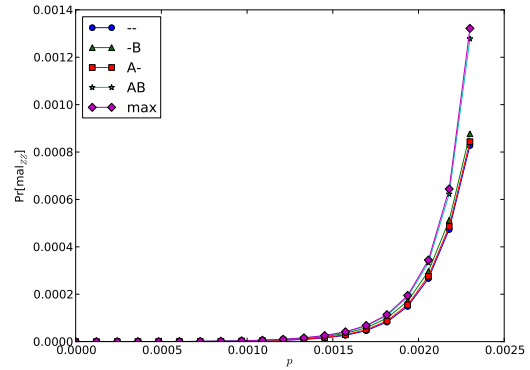
(c)



(d)



(e)



(f)

Figure 17: The above plots show upper bounds on the probability of malignant events for the level-one CNOT exRec where the error corrections are based on Overlap-4 verification schedule. Upper bounds are plotted separately for each of four different CNOT exRecs: the full exRec (labeled AB), and the three incomplete exRecs in which the TEC on block A—the control block—has been removed (-B), the TEC on block B—the target block—has been removed (A-) or the TEC on both blocks have been removed (--). Also shown is the polynomial “max” used to simultaneously upper bound all four possibilities (see [Section 4.4.2](#)).

partial CNOT exRec (see Figure 17). In this case, we require only a single polynomial  $\mathcal{P}^*$  which is strictly greater than or equal to all other polynomials in the set  $P := \{\mathcal{P}_E\}$  over the interval  $[0, \gamma_{\max}]$ . The monotonicity of each of the polynomials (see Section C) over this interval means that constructing a  $\mathcal{P}^*$  is relatively simple. First, choose some reasonably small  $\gamma_{\min} > 0$  and fix some  $\Delta > 0$ . Then a sufficient condition for  $\mathcal{P}^*$  to be greater than all polynomials in  $P$  over the interval  $[\gamma_{\min}, \gamma_{\max}]$  is

$$\mathcal{P}^*(\gamma_{\min} + n\Delta) \geq \mathcal{P}_E(\gamma_{\min} + (n+1)\Delta) \quad (\text{D.3})$$

for all  $\mathcal{P}_E \in P$  and all integers  $0 \leq n \leq \lceil (\gamma_{\max} - \gamma_{\min})/\Delta \rceil$ .  $\mathcal{P}^*$  can be constructed by taking the  $\mathcal{P}_E$  with the largest value at  $\gamma_{\max}$  (say), and adding a constant offset of at least  $\max_E \mathcal{P}_E(\gamma_{\min})$  so that (D.3) is satisfied. Maximality over the remaining interval  $[0, \gamma_{\min}]$  follows by monotonicity.

In the second case, we compare malignant events from different types of exRecs. We need to construct  $\Gamma$  and determine values  $\alpha_E$  for which the upper bound  $\mathcal{P}_E \leq \alpha_E \Gamma$  in (D.1) is satisfied. Construction of  $\Gamma$  is similar to that of  $\mathcal{P}^*$  from above. Let  $\mathcal{P}_j$  be the polynomial with the largest derivative at  $\gamma_{\max}$ . Take  $\mathcal{P}_j$  and divide by some appropriately large value  $r$ . Then add a constant offset  $\epsilon := \max_{i \neq j} \mathcal{P}_i(\gamma_{\min})$  so that  $\Gamma = \mathcal{P}_j/r + \epsilon$ . Finally, for each  $\text{mal}_E$ , find the minimum value of  $\alpha_E$  such that  $\mathcal{P}^* := \alpha_E \Gamma$  satisfies condition (D.3).

In practice, the quality of the resulting bounds depends on the choice of  $\gamma_{\min}$  and the number of plotted points  $n$ . We find that a value of  $\gamma_{\min} = \gamma_{\max}/10$  or  $\gamma_{\min} = \gamma_{\max}/100$ , and  $n = 1000$  works well. More sophisticated methods can also be used. For example, the value of  $\Delta$  could vary over the interval to better capture exponential behavior of the polynomials.

### D.3 Proof of Claim 4.2

We conclude our analysis of the transformed error model by proving Claim 4.2 that the level-two malignant event upper bounds decrease exponentially with  $\gamma$ .

*Proof.* From Appendix A and Appendix D.1 we see that  $\mathcal{P}_E^{(2)}$  is expressed as

$$\frac{\Pr[\text{mal}_E, \text{good}]}{\Pr[\text{accept}]} + \Pr[\text{bad}|\text{accept}] \quad (\text{D.4})$$

The  $\Pr[\text{mal}_E, \text{good}]$  term is expressed as a sum of the form

$$\sum_{k=0}^{k_{\max}} c(k) \Gamma^k \quad (\text{D.5})$$

where all of the coefficients  $c(k)$  are non-negative (because there are no  $XZ$  corrections) and it is understood that  $\Gamma$  is a function of  $\gamma$ . The  $\Pr[\text{accept}]$  term in the denominator is a product of terms of the form

$$1 - \sum_{k=0}^{k_{\max}} c(k) \Gamma^k \quad (\text{D.6})$$

where, again, all  $c(k)$  are non-negative.  $\Pr[\text{bad}|\text{accept}]$  is a sum of terms similar to (D.5), some of which contain (D.6) terms in the denominator.

Due to the strict fault-tolerance of our circuits, the coefficients  $c(k)$  of (D.5) and the numerator coefficients of  $\Pr[\text{bad}|\text{accept}]$  are zero for  $k \leq 3$ . Therefore, for  $0 \leq \epsilon \leq 1$ ,  $\mathcal{P}_E^{(2)}(\epsilon\Gamma)$  is a sum of non-negative terms of the form

$$\frac{\sum_{k=0}^{k_{\max}} c(k)(\epsilon\Gamma)^k}{1 - \sum_{k=0}^{k_{\max}} c(k)(\epsilon\Gamma)^k} \leq \frac{\epsilon^4 \sum_{k=4}^{k_{\max}} c(k)\Gamma^k}{1 - \sum_{k=0}^{k_{\max}} c(k)\Gamma^k} \quad (\text{D.7})$$

which completes the proof. □